AN TOÀN AN NINH THÔNG TIN

Chương trình khóa đào tạo "Bồi dưỡng nâng cao năng lực cho lãnh đạo thông tin trong doanh nghiệp" (CIO) do Bộ Thông tin Truyền thông và Ngân hàng Thế giới tổ chức tại Thành phố Hạ Long, Quảng Ninh từ 21-24/08/2012

Người trình bày: Lê Trung Nghĩa
Văn phòng Phối hợp Phát triển Môi trường Khoa học Công nghệ,
Bộ Khoa học & Công nghệ

Email: letrungnghia.foss@gmail.com
Blogs: http://vn.myblog.yahoo.com/ltnghia
http://vnfoss.blogspot.com/
Trang web CLB PMTDNM Việt Nam: http://vfossa.vn/vi/
HanoiLUG wiki: http://wiki.hanoilug.org/
Đăng ký tham gia HanoiLUG:
http://lists.hanoilug.org/mailman/listinfo/hanoilug/

Mục lục

A. Tổng quan tình hình an toàn an ninh thông tin

1. Một số trích dẫn quan trọng đáng lưu ý

1. Barack Obama, ngày 29/05/2009: "Sự thịnh vượng về kinh tế của nước Mỹ trong thế kỷ 21 sẽ phụ thuộc vào an ninh có hiệu quả của không gian mạng, việc đảm bảo an ninh cho không gian mạng là xương sống mà nó làm nền vững chắc cho một nền kinh tế thịnh vượng, một quân đội và một chính phủ mở, mạnh và hiệu quả". "Trong thế giới ngày nay, các hành động khủng bố có thể tới không chỉ từ một ít những kẻ cực đoan đánh bom tự sát, mà còn từ một vài cái gõ bàn phím trên máy tính – một vũ khí huỷ diệt hàng loạt". Văn bản gốc tiếng Anh. Video.
2. Trích từ tài liệu " An ninh không gian mạng (ANKGM): Câu hỏi gây tranh cãi đối với các qui định toàn cầu", Chương trình Nghị sự về An ninh và Phòng thủ (SDA), xuất bản tháng 02/2012:
    - Isaac Ben-Israel, cố vấn ANKGM cho Thủ tướng Benjamin Netanyahu, Israel: "*Nếu bạn muốn đánh một quốc gia một cách khốc liệt thì bạn hãy đánh vào cung cấp điện và nước của nó. Công nghệ KGM có thể làm điều này mà không cần phải bắn một viên đạn nào*".
    - Phyllis Schneck, Giám đốc công nghệ cho Khu vực Công tại McAfee: "*Công nghệ mới bây giờ được tập trung bên dưới các hệ điều hành. Nó giao tiếp trực tiếp với phần cứng máy tính và các con chip để nhận biết được hành vi độc hại và sẽ đủ thông minh để không cho phép hành vi độc hại đó... Đây là lớp mới nhất và sâu nhất và, cùng với nhiều tri thức hơn trong các lớp khác, là một phần chủ chốt của tương lai ANKGM. Giao tiếp với phần cứng là hoàng hậu của bàn cờ - nó có thể dừng kẻ địch hầu như ngay lập tức hoặc kiểm soát cuộc chơi dài hơn. Cách nào thì chúng ta cũng sẽ thắng*".

    Thông điệp: ANKGM có quan hệ mật thiết với an ninh và sự sống còn của một quốc gia, và nó phụ thuộc vào phần mềm và phần cứng tạo nên hệ thống thông tin được sử dụng trong các hạ tầng sống còn của một quốc gia. Nói một cách khác, an ninh của hệ thống thông tin phụ thuộc trước hết vào kiến trúc của hệ thống thông tin.
3. Trend Macro: Nền công nghiệp chống virus đã lừa dối người sử dụng 20 năm nay. Khả năng chống virus hầu như là không thể với số lượng khổng lồ các virus hiện nay; Năm 2010, cứ mỗi giây có 2 phần mềm độc hại mới được sinh ra, trong khi thời gian nhanh nhất để có được một bản vá lỗi là 3 giờ đồng hồ.
4. McAfee: số lượng các cuộc tấn công bằng phần mềm độc hại để thâm nhập hoặc gây hại cho một hệ thống máy tính tăng 500% trong năm 2008 – tương đương với tổng cộng của 5 năm trước đó cộng lại. Trong đó 80% tất cả các cuộc tấn công bằng phần mềm độc hại có động lực là tài chính, với những kẻ tấn công cố ăn cắp thông tin dữ liệu cá nhân vì lợi nhuận; 20% các cuộc tấn công còn lại có các mục đích liên quan tới tôn giáo, gián điệp, khủng bố hoặc chính trị.

Một vài tư liệu video:

1. Về vụ mạng GhostNet: Video của Symantec; Cyberspies China GhostNet Exposed III; Global Computer Espionage Network Uncovered; China Cyberspy GhostNet targets governments;
2. Tấn công lưới điện Mỹ - China & Russia Infiltrate US Power Grid-Cyber Spies Hack The Grid;
3. Tấn công mạng của Lầu 5 góc - Chinese Military Hacks Pentagon's computer system; Chinese hackers: No site is safe;
4. Tấn công các mạng truyền thông, ngân hàng, điện... của Mỹ - China Cyber Attack on America;

5. Kịch bản sử dụng bộ công cụ để tạo các Zeus botnet phục vụ cho việc ăn cắp tiền trong các tài khoản ngân hàng của các doanh nghiệp.
6. Kịch bản tấn công của Stuxnet.

2. Lý do và mục đích tấn công

1. Về chính trị: không chỉ gián điệp thu thập thông tin, mà còn phá hoại cơ sở hạ tầng.
   a) Xung đột giữa các quốc gia: Israel – Syria, Israel – Palestine, Nga – Estonia, Nga – Georgia (trở thành tiêu chuẩn), Mỹ cùng liên quân – Iraq, Mỹ cùng Hàn Quốc - Bắc Triều Tiên, tranh chấp dầu khí ở Venezuela năm 2002, Mỹ-Israel với Iran.
   b) TQ và các quốc gia khác - 09/10/2009: hàng chục vụ, ở nhiều quốc gia, tần suất gia tăng. Vụ mạng gián điệp thông tin lớn nhất thế giới từ trước tới nay GhostNet: 103 quốc gia, 1295 máy tính bị lây nhiễm, kéo dài từ 05/2007 đến 03/2009.
   c) Tấn công vào hầu như tất cả các hệ thống mạng của các lực lượng vũ trang, như mạng dành riêng cho 2 cuộc chiến tranh mà Mỹ hiện đang tham chiến, CIA, MI6, NATO, Hải quân Ấn Độ; Cảnh sát Anh,
   d) Các tổ chức được cho là mức độ an ninh an toàn hệ thống cao nhất bị tấn công như Thượng viện Mỹ, Thủ tướng Úc, cơ quan chứng thực Israel, Quỹ tiền tệ Quốc tế IMF, Chính phủ Canada, Ủy ban Thương mại Liên bang Mỹ FTC, Bộ Tư pháp Mỹ, Cơ quan Vũ trụ Nhật Bản, Phòng Thương mại Mỹ, Liên hiệp quốc, các vệ tinh quan sát của Mỹ,
   e) Năm 2009 có dự đoán thời gian để chuyển từ gián điệp thông tin sang phá hoại: từ 3-8 năm, trên thực tế đã diễn ra nhanh hơn thế. Ngày 13/07/2010, sâu Windows Stuxnet đã được phát hiện, dựa vào 4 lỗi ngày số 0 trong Windows và các lỗi trong hệ thống kiểm soát giám sát và thu thập dữ liệu SCADA của Siemens, đã làm hỏng hàng ngàn máy li tâm uranium trong các cơ sở hạt nhân của Iran, làm chậm chương trình hạt nhân của nước này tới 2 năm.
   f) Cảnh báo có việc phá hoại hạ tầng cơ sở:
      - Các hệ thống mạng tại Mỹ: lưới điện ([1], [2]), giao thông, ngân hàng, phát thanh truyền hình, đường sắt, cấp thoát nước tại Illinois và Texas, cung cấp dầu khí, công nghiệp hóa chất. Thâm nhập các thiết bị kiểm soát công nghiệp tại Mỹ tăng đột ngột, từ 9 vụ năm 2009 lên 198 vụ năm 2011 với 17 vụ nghiêm trọng;
      - Các nước khác: lưới điện ở Úc, lưới điện Brazil, y tế ở Anh
   g) Stuxnet - Duqu – Flame: Vũ khí không thể kiểm soát, các phần mềm diệt virus bất lực không dò tìm ra được chúng;
   h) WikiLeaks. Vụ nổi tiếng vì đã đưa ra hàng loạt các tài liệu mật của Bộ Quốc phòng và Bộ Ngoại giao Mỹ liên quan tới hàng loạt các quốc gia trên thế giới.
2. Về kinh tế: Gián điệp thu thập thông tin, ăn cắp thông tin sở hữu trí tuệ, ăn cắp tiền.
   a) Các tập đoàn lớn: Sony, Honda, các công ty dầu khí, Lockheed Martin, Citibank, nhà mạng SK Communications - Hàn Quốc, Mitsubishi Heavy Industries - nhà thầu của Bộ Quốc phòng Nhật Bản, vụ Aurora cuối năm 2009 tấn công vào Google và hàng chục hãng lớn khác của Mỹ...
   b) Tháng 08/2012, Kaspersky Lab đã phát hiện một virus mới do nhà nước bảo trợ, Gauss, có liên quan tới Stuxnet-Duqu-Flame, chuyên để theo dõi các giao dịch, dò tìm và ăn cắp các ủy quyền đăng nhập và thông tin - dữ liệu ngân hàng trực tuyến, xuất hiện trong hàng loạt các ngân hàng tại Li băng, Israel và các vùng lãnh thổ của Palestine.

c) Khu vực ngân hàng - thẻ tín dụng: Global Payments với 1.5 triệu thẻ, ăn cắp tiền từ các tài khoản ngân hàng của các doanh nghiệp vừa và nhỏ 40 triệu USD đến tháng 9/2009, 100 triệu USD đến tháng 10/2009, vụ Citibank hàng chục triệu USD, thị trường chứng khoán NASDAQ, ăn cắp tiền thông qua các trò chơi trực tuyến ở Trung Quốc.
d) Các cơ quan chứng thực số CA: Codomo, Diginotar, GlobalSign, StartSSL, làm Diginotar phá sản,
e) Các công ty an ninh và tư vấn an ninh: Stratfor, Symantec...
f) Lừa đảo để bán phần mềm an ninh giả mạo hay tấn công bằng tình dục để tống tiền...

3. Các vụ liên quan tới Việt Nam:
a) Tháng 02/2012, BKAV bị tấn công, nhiều dữ liệu bị lấy cắp. Trong khoảng từ tháng 11/2010 đến tháng 11/2011, Vietnamnet bị tấn công liên tục, lấy và xóa đi nhiều dữ liệu, không tìm ra thủ phạm.
b) Cuộc chiến giữa các tin tặc Việt Nam - Trung Quốc lần thứ nhất, 02-07/06/2011, hàng trăm (hàng ngàn) các website của cả 2 bên đã bị bôi xấu, đánh sập, trong đó có các website của chính phủ.

Chừng nào còn xung đột Biển Đông, chừng đó còn chiến tranh không gian mạng ở Việt Nam!

c) Việt Nam phải hết sức cảnh giác với chiến tranh không gian mạng, đặc biệt đối với các cuộc tấn công vào các cơ sở hạ tầng công nghiệp sống còn kiểu Stuxnet, có thể từ Trung Quốc.
d) GhostNet (số 2/103 nước trên thế giới, chỉ sau Đài Loan, trên cả Mỹ và Ấn Độ), với 130/1295 máy tính chạy Windows bị lây nhiễm (Symantec làm video mô phỏng lại cuộc tấn công), mục đích gián điệp thông tin chống lại các chính phủ, những gì liên quan tới vụ này???, Hiện nay ra sao???;
e) Conficker (Việt Nam đứng số 1 thế giới với 13% số máy bị lây nhiễm theo OpenDNS); Botnet Windows nhiễm Conficker (cả A+B lẫn C) của các ISP Việt Nam cỡ lớn nhất thế giới với hơn 5% không gian địa chỉ IP bị lây nhiễm và vẫn đang tự lây nhiễm. Trong Top500 thế giới: VNN(2), Viettel(18), FPT(20), CMCTI (244), ETC(279), SCTV(302), SPT(398), VNPT(407) theo số liệu tháng 04/2012.
f) Việt Nam có tên ở 5 trong số 10 botnet lớn nhất thế giới vào năm 2009. Việt Nam xếp ở vị trí số 1 ở 4 trong 5 botnet đó (theo một báo cáo vào tháng 06/2010).
g) Tại Việt Nam đã có bộ công tụ Zeus để tạo ra các botnet độc hại.
h) Nháy chuột giả mạo - số 1 thế giới;
i) Mua bán các máy tính bị lây nhiễm trong các botnet trên thi trường tội phạm mạng thế giới, Việt Nam có giá mua vào 5 USD/1000 máy và giá bán ra 25 USD/1000 máy.
j) Màn hình đen (Tại Mỹ, WGA [Windows Genuine Advantage] bị đưa ra tòa vì bị coi như một phần mềm gián điệp); Nay WGA có đổi tên là WAT (Windows Activation Technology).

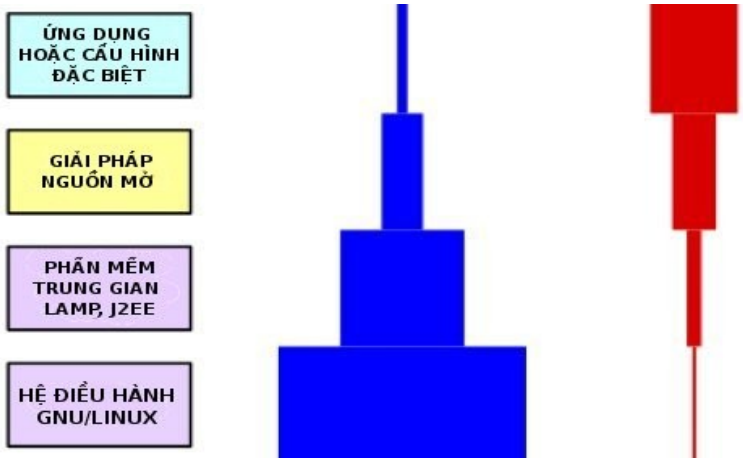
3. Công cụ được sử dụng để tấn công

1. Phần cứng và thiết bị:
a) Chip máy tính, cấy phần mềm độc hại hoặc phần mềm gián điệp vào Bios máy tính (Stoned Boot - tất cả các phiên bản Windows từ XP tới 7, Microsoft làm việc với các OEM để đưa ACPI [Advanced Configuration and Power Interface] vào các máy tính - có thể bị lợi dụng để cấy Trojan vào ngay cả khi đĩa cứng hoàn toàn được mã hóa - bootkit sẽ khởi động trước và tự nó ẩn mình - chiếm quyền kiểm soát toàn bộ máy tính - phải có truy cập vật lý tới máy

tính), lấy dữ liệu khóa an ninh từ DRAM (Cold Boot). Sử dụng các phần mềm độc hại để nao vét RAM, nghe bàn phím, lây nhiễm virus cho các USB để lấy thông tin.

b) Thiết bị viễn thông: vụ thầu thiết bi viễn thông ở Anh, mối quan ngại của Mỹ, Anh, Ấn Độ đối với các thiết bị viễn thông từ công ty Hoa Vĩ (Huwei) hay ZTE của Trung Quốc.
c) Các hệ thống nhúng: các máy photocopy đa chức năng của Canon, Ricoh, Xerox, các thiết bị của CISCO, các máy in của HP ("Bom máy in" làm cho in hết giấy, thâm nhập mang qua máy in)
d) Các thiết bị di động: phần mềm độc hại đang gia tăng nhanh.
e) Thẻ và đầu đọc thẻ thông minh: Bộ Quốc phòng Mỹ.

2. Phần mềm



Lớp ứng dụng **Lượng người sử dụng và độ trưởng thành** **Xác suất lỗi**

a) Xác xuất lỗi được tính theo: (1) Hệ điều hành, (2) Phần mềm trung gian (Middleware), (3) Giải pháp; (4) Phần mềm ứng dụng. Ví dụ, trong phần mềm nguồn mở thì lỗi ở hệ điều hành là ít nhất và tăng dần theo các con số ở trên (với RHEL4.0 và 5.0 thì lỗi mang tính sống còn là bằng 0), còn lượng người sử dụng ở hệ điều hành là lớn nhất rồi giảm dần theo các con số ở trên. (Xem bài "Hỗ trợ nguồn mở" trên tạp chí Tin học và Đời sống, số tháng 11/2009). Nhân của hệ điều hành nguồn mở GNU/Linux được cải tiến, sáng tạo liên tục với tốc độ không thể tưởng tượng được cũng là một điểm rất quan trọng.
b) Cửa hậu được gài trong Windows và một số hệ điều hành thương mại khác và/hoặc trong phần mềm thư điện tử Lotus Notes.
c) Các loại phần mềm độc hại viết cho Windows chiếm tới 99.4% - 99.5% tổng số các phần mềm độc hại được viết ra trên thế giới, theo G-DATA.
d) Tin tặc tận dụng khiếm khuyết của các phần mềm của Microsoft để tấn công các hệ thống mang trên khắp thế giới – Windows, Exchange Server, Office, Wordpad, Internet Explorer... Các phần mềm khác cũng bị lợi dụng để tấn công, phổ biến là của Adobe Acrobat Reader, Adobe Flash, Quicktime, Firefox, AutoCAD, các chương trình SCADA và ICS trên Windows, chương trình cập nhật Windows, ..., các mạng xã hội như Facebook, Twitter...

e) Tạo ra các botnet với các kích cỡ từ nhỏ tới khổng lồ, từ hàng trăm cho tới hàng chục triệu máy tính bị lây nhiễm để chuẩn bị cho các cuộc tấn công qui mô lớn sau này.
f) Các công cụ mã hóa, các chứng thực số, các phần mềm diệt virus bị mở mã nguồn.

3. Thị trường mua bán công cụ tạo mã độc, botnet
   a) Mua bán các trung tâm dữ liệu, mua bán các bộ các công cụ tạo mã độc hại, mã nguồn, để xây dựng các botnet, phần mềm an ninh giả mạo; phần mềm dọa nạt (phishing) đưa người sử dụng vào bẫy để mua phần mềm chống virus giả mạo;
   b) Mua bán máy tính bị lây nhiễm trong các botnet theo vùng địa lý với các thông tin bị ăn cắp đi kèm, giá mua vào từ 5-100 USD/1000 máy bị lây nhiễm cùng dữ liệu bị ăn cắp, giá bán ra từ 25-100 USD.
4. Sử dụng không đúng cách dẫn tới mất an ninh, mất dữ liệu: vụ Sidekick.
5. Pháp nhân tiến hành tấn công: đủ loại, mức cao nhất là nhiều quốc gia tham gia vào chiến tranh KGM như Mỹ, Israel, Trung Quốc, Nga, Anh, ... làm bật dậy cuộc chạy đua vũ trang các vũ khí KGM trên toàn cầu, có khả năng biến KGM thành vùng chiến sự nóng bỏng.

4. Tần suất và phạm vi tấn công

1. Tần suất lớn khổng lồ
   a) Mạng quân đội Mỹ bị quét hàng ngàn lần mỗi ngày.
   b) Tháng 03/2009, có 128 "hành động thâm nhập không gian mạng" trong 1 phút vào các hệ thống mạng của nước Mỹ.
   c) Năm 2010 mỗi giây có 2 phần mềm độc hại mới được sinh ra, trong khi nhanh nhất phải cần tới 3 giờ đồng hồ để có được một bản vá.
2. Phạm vi rộng khắp
   a) Vụ GhostNet tấn công vào 103 quốc gia, 1295 máy tính bị lây nhiễm. Tài liệu 53 trang, video mô tả lại cuộc tấn công.
   b) Các quốc gia mạnh về CNTT cũng bị tấn công: Mỹ, Anh, Pháp, Đức, Hàn Quốc...
   c) Khắp các lĩnh vực như vũ trụ, hàng không, quân sự, tài chính, ngoại giao, ...
3. Nhiều loại sâu, bọ, virus, phần mềm độc hại tham gia các botnet. Có loại chuyên ăn cắp tiền (Zeus, Clampi), có loại tinh vi phức tạp (Conficker), có loại đã tồn tại từ nhiều năm trước nay hoạt động trở lại dù có hàng chục bản vá lỗi của Windows (MyDoom).
4. Thiệt hại lớn
   a) Stuxnet đẩy lùi chương trình hạt nhân của Iran 2 năm mà không tốn viên đạn nào.
   b) Mỹ bị tin tặc lấy đi hàng terabyte dữ liệu từ hệ thống mạng của các Bộ Quốc phòng, Ngoại giao, Thương mại, Năng lượng và Cơ quan Hàng không Vũ trụ NASA.
   c) Obama: Riêng Mỹ, trong 2008-2009 thiệt hại do tội phạm không gian mạng là 8 tỷ USD.
   d) Conficker - ước tính 9.1 tỷ USD chỉ trong nửa năm (tới tháng 6/2009).

5. Đối phó của các quốc gia

1. Về đường lối chính sách:
   a) Học thuyết chiến tranh thông tin, cả phòng thủ lẫn tấn công, bất kỳ vũ khí gì, kể cả hạt nhân; Chiến lược về ANKGM (Mỹ, Anh và nhiều nước khác); Kế hoạch phản ứng (Mỹ). Diễn tập về ANKGM. Hiệp ước cấm phổ biến vũ khí không gian mạng?
   b) Tự chủ về công nghệ lõi. Dự án sản xuất Chip (Trung Quốc, Ấn Độ), chạy đua các dự án

OS tăng cường an ninh như Mỹ (cho Android, Linux, Ethos), Trung Quốc, châu Âu, Úc, hoặc xây dựng mới OS an ninh cho quốc gia mình (Ấn Độ, Nga, Brazil, Venezuela, Cuba …). Tất cả các OS đều dựa trên GNU/Linux/Unix.

c) "Nguồn mở an ninh hơn nguồn đóng" về cả lý thuyết lẫn thực tế do mã nguồn cứng cáp hơn và có được sự rà soát liên tục của cộng đồng các lập trình viên toàn thế giới. Linus Torvalds: "Nói thì ít giá trị, hãy chỉ cho tôi mã nguồn". Hàng loạt chính phủ các quốc gia đã có những chính sách sử dụng công nghệ mở như Mỹ (Chính phủ Mở), Canada, Anh, Hà Lan, Đan Mạch, New Zealand, Malaysia, Ý, Nga, Trung Quốc, Brazil, Ấn Độ, Indonesia, Thailand, Philippine... Trên thế giới, các quốc gia mạnh nhất về ứng dụng và phát triển PMTDNM là Mỹ, Đức, Pháp, Tây Ban Nha và Úc. Năm 2011: Thủ tướng Nga Putin ra lệnh cho các cơ quan chính phủ Nga chuyển hết sang PMTDNM vào quý III/2014; Chính phủ Anh đưa ra Chiến lược công nghệ thông tin và truyền thông của Chính phủ, bắt buộc sử dụng các tiêu chuẩn mở, tăng cường sử dụng PMTDNM ở bất kỳ nơi nào có thể; Bộ Quốc phòng Mỹ đưa ra tài liệu "Phát triển công nghệ mở. Những bài học học được", trong đó nhấn mạnh các phần mềm/hệ thống trong quân đội và chính phủ sẽ không tồn tại phần mềm sở hữu độc quyền chỉ phụ thuộc vào một nhà cung cấp, chỉ có 2 loại là PMTDNM và PMNM chính phủ. Phương châm của phát triển công nghệ mở là: (1) Cộng đồng trước, công nghệ sau; (2) Mở là mặc định, đóng chỉ khi cần thiết; (3) Chương trình của bạn không phải là đặc biệt, thậm chí là trong các dự án phần mềm/hệ thống quân sự về CNTT.

d) Đầu tư lớn vào các nghiên cứu về an ninh KGM. Sản xuất các vũ khí mới cho chiến tranh không gian mạng: "bom logic", các thiết bị sóng cực ngắn để đốt các máy tính trong mạng từ xa; tạo các "botnet"...

2. Về tổ chức: Bổ nhiệm lãnh đạo ANKGM (Mỹ), củng cố và xây dựng lực lượng chuyên môn (Mỹ, Anh, Hàn Quốc, Singapore), các đơn vị ứng cứu khẩn cấp (CERT) quốc gia, hợp tác các CERT và tham gia diễn tập giữa các quốc gia, tăng cường nhân lực và đầu tư cho các cơ quan chuyên trách (Bộ An ninh Quốc nội - DHS, Cục Tình báo Trung ương - CIA, ...).
3. Về nhân lực: Huy động thanh niên, học sinh, sinh viên. Mỹ tổ chức thi để lấy 10,000 nhân tài, Anh cũng bước theo, Bộ An ninh Quốc nội Mỹ tuyển 1,000 nhân viên làm về an ninh không gian mạng. Trung Quốc có "Quân đội xanh", phong trào thanh niên Nga... Bọn khủng bố cũng tuyển người cho chiến trang không gian mạng.
4. Về thực tiễn triển khai khu vực dân sự để đảm bảo an ninh cao
   a) Chuyển sang sử dụng các hệ thống dựa trên GNU/Linux (Thị trường chứng khoán ở New York, Tokyo, Luân Đôn, …)
   b) Không sử dụng Windows khi thực hiện các giao dịch ngân hàng trực tuyến (khuyến cáo của Viện Công nghệ SAN, chính quyền New South Wale – Úc, chuyên gia an ninh mạng của tờ The Washington Post).v.v.
   c) Hàng chục công cụ an ninh từ các phần mềm tự do nguồn mở ([01], [02]).
   d) Khuyến cáo sử dụng PMTDNM, nhưng nếu buộc phải sử dụng Windows, thì hãy tuân thủ 10 lời khuyên về an ninh.

6. Bài học cho Việt Nam

1. Các cơ quan, doanh nghiệp đối mặt với các mối đe dọa an ninh không gian mạng (KGM) với các đặc tính chưa từng có trước đây:

a) Không cần có tiếp xúc vật lý tới các mục tiêu tấn công khi tấn công trên KGM.
b) Công nghệ cho phép các hoạt động diễn ra dễ dàng xuyên biên giới nhiều nước.
c) Có thể tấn công một cách tự động, tốc độ cao, số lượng lớn các nạn nhân cùng một lúc.
d) Những kẻ tấn công dễ dàng dấu mặt.

2. Nguy cơ phụ thuộc, mất kiểm soát hoàn toàn: Việt Nam hiện đang bị phụ thuộc hoàn toàn vào phần cứng, hệ điều hành, phần mềm ứng dụng, có thể sẽ phụ thuộc nốt cả dữ liệu. Hiện vẫn còn cơ hội, dù rất nhỏ, để thoát???
   a) Trước mắt: Chuẩn mở và hệ điều hành nguồn mở (Viettel, Google) là mục tiêu số 1?. Cách chống virus tốt nhất là sử dụng hệ điều hành GNU/Linux. Hiện tại các doanh nghiệp Việt Nam đứng thứ 75/75 về các hoạt động liên quan tới nguồn mở theo nghiên cứu của RedHat-Georgia tháng 04/2009.
   b) Tương lai: Hệ điều hành, chip, các thiết bị viễn thông... **Cần làm chủ được CNTT**.
3. Các lĩnh vực an ninh KGM cần tập trung quan tâm
   a) Đẩy mạnh phân tích KGM và các khả năng cảnh báo.
   b) Cải thiện an ninh KGM mạng các hệ thống kiểm soát hạ tầng.
   c) Tăng cường khả năng của các cơ quan chuyên trách để giúp phục hồi từ phá hoại Internet.
   d) Giảm thiểu sự không hiệu quả về tổ chức.
   e) Xác định đầy đủ các hành động qua thực tiễn về an ninh KGM.
   f) Phát triển các kế hoạch đặc thù cho từng khu vực với các tiêu chí về an ninh KGM.
   g) Đảm bảo an ninh các hệ thống thông tin nội bộ.
      - Tuân thủ kiến trúc phân vùng mạng, tuân thủ kiểm soát truy cập các vùng mạng, tuân thủ các yêu cầu cơ bản đảm bảo an ninh mạng.
      - Tuân thủ chuẩn an ninh mạng, ứng dụng, như bộ các chuẩn ISO/IEC 27K, trong đó có ISO/IEC 27032: Các chỉ dẫn cho an ninh không gian mạng.
      - Nhanh chóng áp dụng công nghệ mở.
4. Về chính sách, chiến lược:
   a) Rà soát lại chính sách về các chuẩn sử dụng trong các HTTT nhà nước, kiên quyết sử dụng các chuẩn mở; hướng tới hệ điều hành nguồn mở cộng đồng.
   b) Rà soát lại chính sách mua sắm của chính phủ, tiếp tục triển khai chính sách về ứng dụng phần mềm tự do nguồn mở, đưa ra chính sách riêng cho an ninh KGM.
   c) Quy hoạch an toàn và an ninh số quốc gia – Quyết định số 63/2010/QĐ-TTg
5. Về tổ chức và xây dựng lực lượng:
   a) Xây dựng và củng cố bộ máy phù hợp để đối phó với an ninh KGM.
   b) Học tập các kinh nghiệm về an ninh KGM để vận dụng trong thực tế của Việt Nam.
   c) Đầu tư mạnh mẽ cho giáo dục để chuẩn bị nhân lực cho tương lai từ học sinh - sinh viên, với các kỹ năng mới dựa trên công nghệ mở, phần mềm tự do nguồn mở, các sáng kiến biến các trò chơi điện tử thành các bài học về an ninh.
6. Phòng ngừa cho bản thân, đặc biệt với các máy tính xách tay, kể cả khi mã hóa cả ổ cứng.
7. Nâng cao nhận thức cho toàn xã hội, cuộc chiến của toàn dân, các CIO phải đi đầu làm gương.

B. Giới thiệu một số tiêu chuẩn về an toàn an ninh thông tin

1. Một số tiêu chuẩn về hệ thống quản lý an ninh thông tin ISMS

Hiện tại, trên thế giới hiện đang tồn tại một họ các tiêu chuẩn 27K của Cơ quan tiêu chuẩn hóa quốc tế ISO, gồm khoảng 30 tiêu chuẩn, trong số đó có

Các tiêu chuẩn đã được ban hành

1. ISO/IEC 27000:2009. Các ISMS (Information Security Management System) - Các nguyên lý cơ bản và thuật ngữ.
2. ISO/IEC 27001:2005. Đặc tả về ISMS. Đã có TCVN ISO/IEC 27001:2009.
3. ISO/IEC 27002:2005. Mã thực hành đối với Quản lý An ninh Thông tin.
4. ISO/IEC 27003:2010. Chỉ dẫn triển khai ISMS.
5. ISO/IEC 27004:2009. Quản lý an ninh thông tin - Đo lường.
6. ISO/IEC 27005:2008. Quản lý rủi ro an ninh thông tin.
7. ISO/IEC 27006:2007. Các yêu cầu đối với các cơ quan cung cấp kiểm toán và chứng chỉ các ISMS.
8. ISO 27799:2008. Công nghệ thông tin trong y tế - Quản lý an ninh thông tin trong y tế bằng việc sử dụng ISO/IEC 27002.
9. ISO/IEC 27007:2011. Các chỉ dẫn về việc kiểm toán ISMS.
10. ISO/IEC TR 27008:2011. Chỉ dẫn cho các nhà kiểm toán về kiểm soát ISMS.
11. ISO/IEC 27010:2012. Quản lý an ninh thông tin đối với truyền thông liên lĩnh vực, liên tổ chức.

Các tiêu chuẩn sẽ được ban hành trong thời gian tới

12. ISO/IEC 27013. Chỉ dẫn về triển khai tích hợp các ISO/IEC 20000-1 và ISO/IEC 27001 (dự thảo).
13. ISO/IEC 27014. Khung công việc chế ngự an ninh thông tin (dự thảo).
14. ISO/IEC 27015. Các chỉ dẫn của các ISMS cho khu vực tài chính và bảo hiểm (dự thảo).
15. ISO/IEC 27017. An ninh trong điện toán đám mây (dự thảo).
16. ISO/IEC 27018. Quy phạm cho các kiểm soát bảo vệ dữ liệu đối với các dịch vụ điện toán đám mây công cộng (dự thảo).
17. ISO/IEC 27031. Các chỉ dẫn về tính sẵn sàng về ICT cho tính liên tục của công việc (bản thảo cuối).
18. ISO/IEC 27032. Các chỉ dẫn cho an ninh không gian mạng (CD).
19. ISO/IEC 27033. An ninh mạng (dự thảo).
20. ISO/IEC 27034. An ninh các ứng dụng (dự thảo).
21. ISO/IEC 27035. Quản lý sự cố an ninh (dự thảo).
22. ISO/IEC 27036. Các chỉ dẫn về an ninh thuê ngoài làm (dự thảo).
23. ISO/IEC 27037. Các chỉ dẫn về nhận diện, thu thập và/hoặc thu được và gìn giữ bằng chứng số (dự thảo).

24. ISO/IEC 27039. Lựa chọn, triển khai và vận hành các hệ thống dò tìm thâm nhập trái phép - IDPS (Intrusion Detection [and Prevention] System) (dự thảo).
25. ISO/IEC 27040. An ninh lưu giữ (dự thảo).
26. ISO/IEC 27041. Chỉ dẫn cho việc đảm bảo tính bền vững và đầy đủ của các phương pháp điều tra (dự thảo).
27. ISO/IEC 27042. Chỉ dẫn cho việc phân tích và giải nghĩa bằng chứng số (dự thảo).
28. ISO/IEC 27043. Các nguyên tắc và qui trình điều tra bằng chứng số (dự thảo).

Chưa có nhiều doanh nghiệp trên thế giới có chứng chỉ tuân thủ các chuẩn ISO/IEC 27K về ISMS và rất tốn kém để có thể đạt được chúng (có thể lên tới hàng trăm ngàn USD).
Xem http://www.iso27001security.com/html/iso27000.html để biết chi tiết hơn về họ các tiêu chuẩn ISO/IEC 27K.

2. Một số tiêu chuẩn cho điện toán đám mây

Vì ĐTĐM là mới, nên còn thiếu nhiều tiêu chuẩn, kể cả về an ninh, tính tương hợp, tính khả chuyển và tính riêng tư.

2.1. Tiêu chuẩn về an ninh

Bảng dưới đây ánh xạ các tiêu chuẩn cho các chủng loại an ninh trong Nguyên tắc phân loại ĐTĐM của NIST và đưa ra tình trạng về độ chín của tiêu chuẩn. Một số trong số các tiêu chuẩn được liệt kê áp dụng cho hơn một chủng loại và vì thế được liệt kê hơn một lần.

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
Xác thực & Ủy quyền	RFC 5246: Secure Sockets Layer (SSL)/ Transport Layer Security (TLS); IETF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	RFC 3820: X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile; IETF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	RFC5280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; IETF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	RFC 5849: Oauth (Open Authorization Protocol); IETF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
	OpenID Authentication; OpenID	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	eXtensible Access Control Markup Language (XACML); OASIS	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	Security Assertion Markup Language (SAML); OASIS	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 181: Automated Password Generator; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 190: Guideline for the Use of Advanced Authentication Technology Alternatives; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 196: Entity Authentication Using Public Key Cryptography; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
Tính bí mật	RFC 5246: Secure Sockets Layer (SSL)/ Transport Layer Security (TLS); IETF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	Key Management Interoperability Protocol (KMIP); OASIS	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	XML Encryption Syntax and Processing; W3C	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 140-2: Security Requirements for Cryptographic Modules; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 185: Escrowed Encryption Standard (EES); NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 197: Advanced Encryption Standard (AES); NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 188: Standard Security Label for Information Transfer; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
Tính toàn vẹn	XML signature (XMLDSig); W3C	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 180-3: Secure Hash Standard (SHS); NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 186-3: Digital Signature Standard (DSS); NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC); NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
Quản lý nhận diện	Service Provisioning Markup Language (SPML); WSFederation and WS-Trust	Tiêu chuẩn được phê chuẩn
	X.idmcc – Requirement of IdM in Cloud Computing, ITU-T	Đang phát triển
	Security Assertion Markup Language (SAML); OASIS	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	OpenID Authentication, OpenID Foundation	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
An ninh	NIST SP 800-126: Security Content Automation Protocol (SCAP), NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	NIST SP 800-61 Computer Security Incident Handling Guide, NIST	Tiêu chuẩn được phê chuẩn
	X.1500 Cybersecurity information exchange techniques, ITU-T	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	X.1520: Common vulnerabilities and exposures; ITU-T	Tiêu chuẩn được phê chuẩn
	X.1521; Common Vulnerability Scoring System; ITU-T	Tiêu chuẩn được phê chuẩn

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
	PCI Data Security Standard; PCI	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 191: Guideline for the Analysis of Local Area Network Security; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
Quản lý chính sách an ninh	eXtensible Access Control Markup Language (XACML); OASIS	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 199: Standards for Security Categorization of Federal Information and Information Systems; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	FIPS 200: Minimum Security Requirements for Federal Information and Information Systems; NIST	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
Tính sẵn sàng	Availability ISO/PAS 22399:2007 Guidelines for incident preparedness and operational continuity management, ISO	Chấp nhận của thị trường

Bảng 1 - An ninh: Phân loại

2.2. Tiêu chuẩn về tính tương hợp

Tính tương hợp của các dịch vụ đám mây có thể được phân loại theo các giao diện quản lý và chức năng của các dịch vụ đám mây. Nhiều tiêu chuẩn CNTT đang tồn tại đóng góp cho tính tương hợp giữa các ứng dụng đám mây của người sử dụng và dịch vụ đám mây, và giữa bản thân các dịch vụ đám mây. Có những nỗ lực tiêu chuẩn hóa đặc biệt được khởi xướng để giải quyết những vấn đề về tính tương hợp trong đám mây. Những tiêu chuẩn đám mây đặc biệt này được liệt kê trong Bảng sau.

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
Tính tương hợp dịch vụ	Open Cloud Computing Interface (OCCI); Open Grid Forum	Tiêu chuẩn được phê chuẩn
	Cloud Data Management Interface (CDMI); Storage Networking Industry Association, SNIA	Tiêu chuẩn được phê chuẩn
	IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP), IEEE	Đang phát triển

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
	IEEE P2302, Draft Standard for Intercloud Interoperability and Federation (SIIF), IEEE	Đang phát triển

Bảng 2 - Tính tương hợp: Phân loại

2.3. Tiêu chuẩn về tính khả chuyển

Các vấn đề về tính khả chuyển trong đám mây bao gồm tính khả chuyển về tải công việc và các dữ liệu. Trong khi một số vấn đề về tính khả chuyển của tải công việc đám mây là mới, thì nhiều tiêu chuẩn cho dữ liệu và siêu dữ liệu hiện đang tồn tại đã được phát triển trước kỷ nguyên đám mây. Bảng sau đây tập trung vào các tiêu chuẩn về tính khả chuyển đặc thù của đám mây.

Chủng loại	Các tiêu chuẩn và SDO sẵn sàng	Tình trạng
Tính khả chuyển về dữ liệu	Cloud Data Management Interface (CDMI); SNIA	Tiêu chuẩn được phê chuẩn
Tính khả chuyển về hệ thống	Open Virtualization Format (OVF); DMTF	Tiêu chuẩn được phê chuẩn Chấp nhận của thị trường
	IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP), IEEE	Đang phát triển

Bảng 3 - Tính khả chuyển: Phân loại

Chi tiết hơn về các tiêu chuẩn trong ĐTĐM, xem: "Lộ trình tiêu chuẩn Điện toán Đám mây của NIST v1.0", Viện Tiêu chuẩn và Công nghệ Quốc gia, Mỹ - NIST. Tháng 07/2011. 76 trang. Các tác giả: Michael Hogan, Fang Liu, Annie Sokol, Jin Tong.

URL: http://ubuntuone.com/3n18xI3STBrnAZ3VnjrCrp

3. Một số tiêu chuẩn theo mô hình kiến trúc an ninh dữ liệu

Cần có một số qui định chính thức của Chính phủ về hệ thống quản lý an ninh thông tin của riêng mình, có thể dựa vào tiêu chuẩn ISO/IEC 27001 đã được chuyển sang TCVN để làm cơ sở cho các vấn đề và khái niệm có liên quan và được các bên tham gia liên tục đóng góp ý kiến phản hồi trong quá trình triển khai thực tế.

Dưới đây là một vài tiêu chuẩn theo kiến trúc về mô hình cho các chuẩn an ninh dữ liệu có tính gợi ý:

1. Triển khai khái niệm an ninh: Đặc tả Tính tương hợp Chữ ký Công nghiệp - MailTrusT (ISIS-MTT) v1.1. Tài liệu gốc của đặc tả ISIS-MTT cấu tạo từ 8 phần với các nội dung sau:

- Việc thiết lập các chứng thực khóa công khai, các chứng thực thuộc tính và các danh sách thu hồi chứng thực
- Thiết lập và gửi các yêu cầu cho cơ quan chứng thực (PKCS#10) và những trả lời từ cơ quan chứng thực (PKCS#7)
- Thiết lập các thông điệp được mã hóa và được ký
- Các yêu cầu cho các chứng thực khóa công khai, các chứng thực thuộc tính và các danh sách thu hồi chứng thực có sử dụng LDAP, OCSP[1], FTP hoặc HTTP; thiết lập các câu hỏi và đáp và từ các đơn vị đóng dấu thời gian.
- Kiểm tra tính hợp lệ cho các chứng thực khóa công khai và các chứng thực thuộc tính
- Các thuật toán được phê chuẩn cho các hàm băm, các chữ ký, mã hóa, xác thực các thông điệp tới và từ cơ quan chứng thực; các thuật toán được phê chuẩn cho Chữ ký XML và Mã hóa XML.
- Mô tả "Giao diện thẻ Token Mật mã" (PKCS#11) với các dạng và chức năng của dữ liệu
- Lập hồ sơ và mở rộng các chữ ký XML và mã hóa XML

2. Phương pháp mã hóa không đối xứng: RSA
3. Phương pháp mã hóa đối xứng: Tiêu chuẩn mã hóa tiên tiến AES (Advanced Encryption Standard).
4. Dữ liệu băm: Thuật toán băm an ninh: (SHA) - 256 (Secure Hash Algorithm).
5. Quản lý khóa: Đặc tả Quản lý Khóa XML (XKMS) v2 (XML Key Management Specification)
6. Thẻ thông minh tiếp xúc: Các thẻ nhận diện - Các thẻ mạch tích hợp (Identification Cards - Integrated circuit cards).
7. Thẻ thông minh không tiếp xúc: Các thẻ Nhận diện - Các thẻ mạch tích hợp không tiếp xúc (Identification Cards - Contactless Integrated Circuit Cards).

Chi tiết hơn, xem: Chuẩn và kiến trúc cho các ứng dụng CPĐT, phiên bản 4.0, Bộ Nội vụ Cộng hòa Liên bang Đức phối hợp với Viện Fraunhofer về phần mềm và kỹ thuật hệ thống (ISST) xuất bản, tháng 03/2008.

1 OCSP = Giao thức Tình trạng Chứng thực Trực tuyến (Online Certificate Status Protocol)

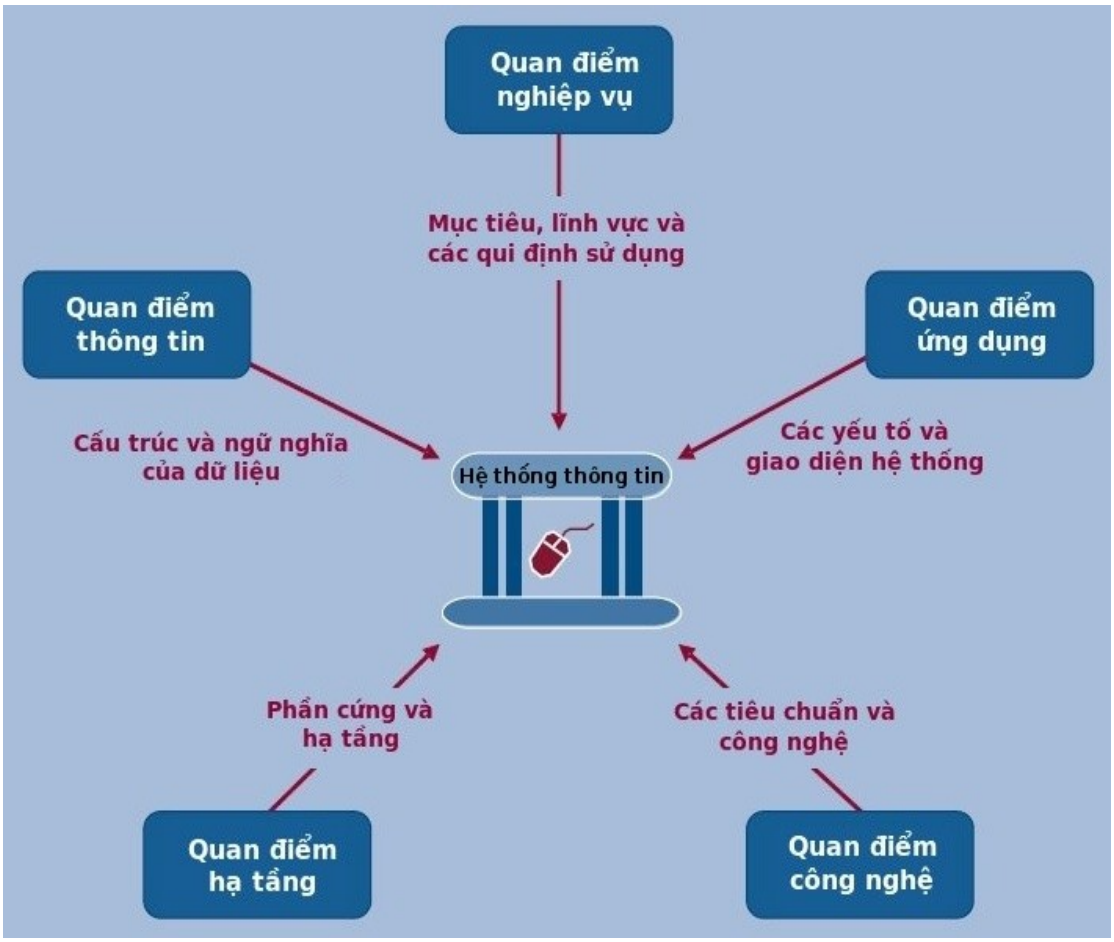
C. Các giải pháp, công cụ và các lỗ hổng thường gặp

Một hệ thống thông tin được cấu tạo từ phần cứng, các thiết bị viễn thông, phần mềm và các dữ liệu trong hệ thống đó. Để đảm bảo an toàn an ninh cho hệ thống, ít nhất, cần hiểu và làm chủ được toàn bộ kiến trúc của hệ thống đó. Bên cạnh đó, còn cần hiểu những vấn đề khác có liên quan tới an toàn an ninh hệ thống, ví dụ như các cách thức quản lý, điều hành và/hoặc những đặc thù của hệ thống đó.

Dưới đây trình bày ví dụ về kiến trúc tổng thể của một hệ thống thông tin và các thành phần của nó.

1. Kiến trúc hệ thống thông tin truyền thông (CNTT – TT)

Kiến trúc một hệ thống công nghệ thông tin và truyền thông (CNTT-TT), dựa vào nó mà một hệ thống CNTT-TT được xây dựng thường bao gồm những lớp cơ bản là: lớp nghiệp vụ, lớp thông tin, lớp hạ tầng, lớp ứng dụng và lớp công nghệ.



Các biện pháp để đảm bảo an ninh hệ thống và thông tin, dữ liệu được tiến hành thực hiện xuyên suốt tất cả các lớp. Tương tự, việc chuẩn hóa dữ liệu cũng được tiến hành thực hiện theo tất cả các lớp.

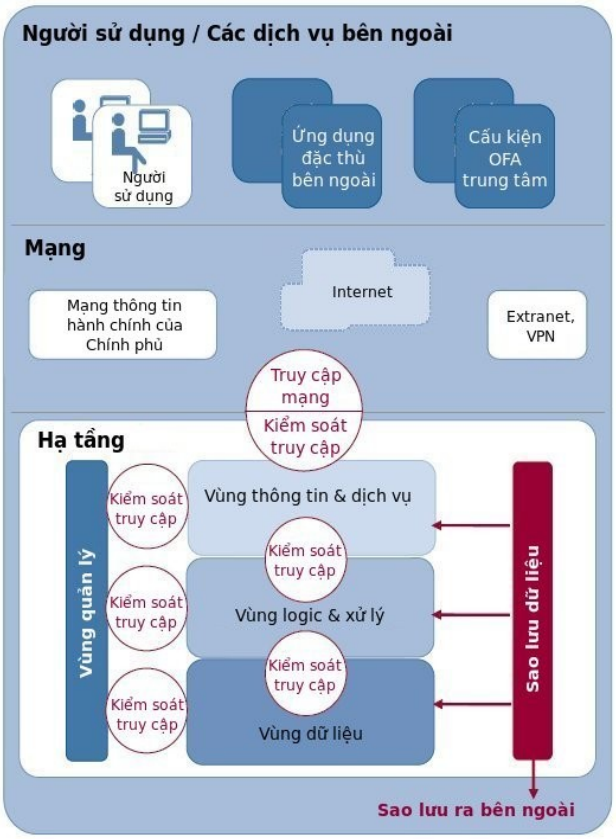
2. An ninh hạ tầng hệ thống CNTT-TT

1. An ninh hệ thống và thông tin, dữ liệu có quan hệ chặt chẽ với việc chuẩn hóa, chọn các bộ chuẩn và ngược lại.
2. Hạ tầng công nghệ thông tin và truyền thông an ninh và ổn định là điều kiện cơ bản tiên quyết cho việc vận hành một cách tin cậy các ứng dụng của một hệ thống thông tin.
3. Bên cạnh việc phải đảm bảo hạ tầng vật lý của hệ thống mạng thì nguyên lý xây dựng hạ tầng CNTT-TT an ninh và ổn định nằm ở việc phân vùng chức năng và đảm bảo an ninh cho việc truy cập các vùng chức năng đó.

Hạ tầng vật lý của hệ thống CNTT-TT

Hạ tầng vật lý của hệ thống CNTT-TT cần được đảm bảo:

1. Thiết lập các hệ thống CNTT trong các phòng phù hợp
2. Kiểm soát truy cập tới các phòng này
3. Các hệ thống bảo vệ phòng và chữa cháy phù hợp
4. Các hệ thống cung cấp điện phù hợp
5. Các hệ thống điều hoà không khí phù hợp
6. Sao lưu dữ liệu theo khái niệm sao lưu dữ liệu liên quan



Kiến trúc hạ tầng và việc đảm bảo an ninh truy cập các vùng

Vùng và các mối giao tiếp

Các hệ thống bên trong trung tâm máy tính được đặt trong các vùng khác nhau được xác định trên cơ sở các yêu cầu về an ninh phù hợp cho các dịch vụ và dữ liệu của các vùng tương ứng đó. Ít nhất những vùng được mô tả dưới đây phải được triển khai trong hạ tầng của một trung tâm máy tính. Có thể đòi hỏi các vùng bổ sung khi cần. Các vùng này phải được tách biệt hoàn toàn với nhau về vật lý. Điều này có thể có nghĩa là:

- Mọi thành phần mạng (bộ định tuyến router, bộ chuyển mạch switch, bộ chia hub, ...) chỉ có thể được sử dụng như là giao diện giữa vùng này với vùng khác, sao cho mọi thành phần mạng chỉ truyền dữ liệu liên quan hoặc dữ liệu gốc qua 2 vùng kết nối trực tiếp với nó. Điều này tránh được mọi sự trộn lẫn các luồng dữ liệu trong trường hợp có lỗi hoặc bị tấn công có chủ tâm.
- Một hệ thống máy chủ có thể chứa các hệ thống của chỉ một vùng duy nhất. Điều này có nghĩa là các ứng dụng phân tán phải chạy trên các hệ thống máy chủ trong các vùng khác nhau.
- Một hệ thống máy chủ với các ứng dụng đòi hỏi các kết nối giao tiếp tới một vài vùng phải bao gồm một số lượng tương ứng các kết nối mạng được tách biệt nhau cả về mặt logic lẫn về mặt vật lý (ví dụ, nhiều card mạng). Hệ thống này sẽ loại trừ được sự truyền từ một vùng này sang một vùng khác.

1. Vùng thông tin và dịch vụ
   a) Vùng thông tin và các dịch vụ bao trùm một phần mạng nằm giữa vùng Internet và các vùng khác của mạng. Vùng này chứa các máy chủ có thể truy cập được bởi các mạng bên ngoài hoặc sử dụng các dịch vụ của các mạng bên ngoài. Các vùng thông tin tiếp sau phải được thiết lập nếu các hệ thống với các mức an ninh khác nhau được vận hành.
   b) Việc giao tiếp giữa các hệ thống của vùng thông tin và dịch vụ cũng như các hệ thống của vùng xử lý và logic phải được bảo vệ bằng các kênh giao tiếp có mã hoá.
2. Vùng xử lý và logic: Các hệ thống của vùng này xử lý dữ liệu từ vùng dữ liệu và làm cho các dữ liệu như vậy sẵn sàng phục vụ người sử dụng thông qua các hệ thống của vùng thông tin và các dịch vụ. Giao tiếp trực tiếp giữa các mạng bên ngoài – như Internet chẳng hạn – và vùng xử lý và logic là không được phép.
3. Vùng dữ liệu: Vùng dữ liệu là nơi mà các dữ liệu được lưu trữ và sẵn sàng trong một khoảng thời gian dài. Việc truy cập tới vùng này chỉ được cho phép từ vùng xử lý và vùng quản trị. Việc truy cập từ các mạng bên ngoài là không được phép trong mọi tình huống. Hơn nữa, chỉ có vùng quản trị mới có thể truy cập một cách tích cực được tới vùng này.
4. Vùng quản trị
   a) Vùng quản trị có tất cả các hệ thống cần thiết cho các mục đích quản trị hoặc các hệ thống giám sát trong các vùng khác. Hơn nữa, vùng này cũng có thể chứa các dịch vụ đăng nhập hoặc quản trị người sử dụng một cách tập trung. Truy cập từ vùng quản trị tới các vùng khác và ngược lại vì thế là được phép.
   b) Truy cập từ các mạng bên ngoài tới vùng quản trị không được phép dưới mọi hình thức.
5. Vùng sao lưu dữ liệu: Mọi vùng phải chứa các thành phần sao lưu dữ liệu của chính vùng đó. Dữ liệu của các vùng thông tin phải được sao lưu thông qua các kênh giao tiếp được bảo vệ.

Chuẩn cho sự tuân thủ an ninh mạng: ISO/IEC 27033: An ninh mạng (dự thảo).

Truy cập mạng và kiểm soát truy cập

1. Các hệ thống kiểm soát truy cập sẽ kiểm soát sự tách biệt của các vùng riêng rẽ bên trong trung tâm máy tính cũng như việc truy cập từ và/hoặc tới các mạng bên ngoài. Các công nghệ khác nhau có thể được sử dụng cho các mục đích này.
2. Giao diện giữa vùng thông tin và các dịch vụ và các mạng bên ngoài là điểm an ninh sống còn nhất và vì thế được bảo vệ bởi một tổ hợp đa cơ chế an ninh (multiple securrity mechnism). Các phân đoạn mạng và các vùng địa chỉ khác nhau được tách biệt nhau ở đây trên mức giao thức mạng. Các địa chỉ mạng bên trong được đánh mặt nạ (mask) theo các mạng dựa trên giao thức TCP/IP trên cơ sở giao thức dịch địa chỉ mạng NAT (Network Address Translation), và vì thế không được xuất bản trong các mạng bên ngoài.
3. Hơn nữa, các cơ chế lọc sẵn có được đưa vào để đảm bảo là việc truy cập từ các mạng bên ngoài bị hạn chế đối với các dịch vụ xác định trong vùng thông tin và các dịch vụ. Các qui định lọc thường được triển khai trên các tường lửa hoặc các bộ định tuyến của tường lửa mà chúng kiểm tra thông tin trong các đầu đề (header) của các gói dữ liệu đến trên cơ sở các bộ lọc gói và từ chối các cuộc tấn công truy cập không được xác thực cho phép.
4. Hơn nữa, các cổng (gateway) vào các ứng dụng có thể được sử dụng để cách ly hoàn toàn các giao tiếp, kiểm tra tính đúng đắn của các dòng dữ liệu ở mức ứng dụng và khi cần thiết sẽ triển khai việc tái sinh lại một cách phù hợp với giao thức của các yêu cầu.
5. Quan hệ giao tiếp giữa các vùng bên trong cũng phải tuân theo các hệ thống kiểm soát truy cập. Để kiểm soát một cách thích đáng việc truy cập tới các vùng nhạy cảm của vùng xử lý và logic cũng như vùng dữ liệu, các tường lửa phải được sử dụng vì chúng có những lựa chọn lọc hỗn hợp. Các tường lửa này làm việc trên cơ sở các bộ lọc gói động (kiểm soát theo trạng thái) và có khả năng giám sát không chỉ các gói đơn lẻ, mà còn cả các dòng giao tiếp liên quan tới nhiều gói. Các bộ lọc gói động cho phép kiểm tra tính hợp lệ của các kết nối mạng không chỉ trên cơ sở các qui tắc không thay đổi mà còn cả trên cơ sở các quan hệ giao tiếp có tính lịch sử.
6. Nhờ việc quản trị đơn giản và mềm dẻo, công nghệ VLAN là hệ thống được chọn cho việc kiểm soát truy cập tới các hệ thống trong vùng quản trị. Vì mục đích này, tất cả các hệ thống đòi hỏi truy cập tới một dịch vụ trong vùng quản trị được tổng hợp để tạo ra một phân mạng ảo (VLAN). Để tránh giao tiếp không mong muốn giữa các vùng riêng biệt thông qua các VLAN của vùng quản trị, tất cả các hệ thống được lắp đặt một giao diện mạng thứ hai mà giao diện này có thể không được sử dụng cho bất kỳ mục đích nào khác ngoài mục đích quản trị và nó được lắp với một bộ lọc gói.
7. Việc sử dụng công nghệ VLAN cho việc kết nối mọi vùng ngoại trừ quản trị không được khuyến cáo vì các lý do an ninh.

Mạng, người sử dụng và các dịch vụ bên ngoài

1. Mức mạng là kết nối giữa các hệ thống của hạ tầng trung tâm máy tính và các dịch vụ bên ngoài cũng như những người sử dụng các ứng dụng CPĐT. Mức này bao gồm cả Internet, mạng diện rộng chính phủ (CPNET) và các mạng extranet khác. Các mạng intranet nội bộ cũng tạo nên một phần của mức mạng. Hiện nay có thể tồn tại nhiều công nghệ khác nhau đang được sử dụng. Về lâu dài, nên lựa chọn các giao thức có khả năng làm cho hệ thống có tính tương hợp.
2. Tuy nhiên, từ quan điểm hạ tầng đối với một ứng dụng CPĐT, giao tiếp an toàn và thực thi với Internet, thì CPNET hoặc extranet đóng một vai trò quan trọng để đảm bảo việc truy cập tin cậy đối với người sử dụng và các dịch vụ bên ngoài. Khi thiết kế các ứng dụng CPĐT, độ rộng băng thông

cần thiết để có thể vận hành và truy cập dễ dàng được các ứng dụng, dịch vụ cần được lưu tâm tới.

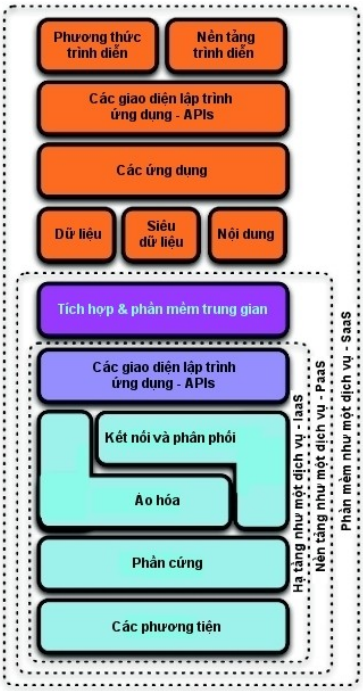
3. An ninh ứng dụng

Kiến trúc ứng dụng theo mô hình đa tầng

Các ứng dụng cần được xây dựng theo kiến trúc phân tầng sao cho có sự tách biệt nhau giữa các tầng nền tảng/phụ trợ (hệ điều hành, hệ quản trị cơ sở dữ liệu, ...), tầng trung gian (qui trình nghiệp vụ và các thành phần tích hợp), tầng trình diễn (trình bày thông tin, dữ liệu), tầng máy trạm (các công cụ của máy trạm giúp cho việc truy cập/hiển thị/xử lý thông tin, dữ liệu của ứng dụng). Bằng cách này, việc đảm bảo an ninh cũng được thực hiện theo các tầng tương ứng.

Chuẩn về an ninh ứng dụng ISO/IEC 27034: An ninh ứng dụng (dự thảo).

4. An ninh điện toán đám mây (ĐTĐM)



An ninh ĐTĐM (an ninh đám mây) là một lĩnh vực tiến hóa của an ninh máy tính, an ninh mạng và, ở mức độ rộng lớn hơn, an ninh thông tin. Nó tham chiếu tới một tập hợp lớn các chính sách, các công nghệ, và những kiểm soát được triển khai để bảo vệ các dự liệu, các ứng dụng và hạ tầng có liên quan tới ĐTĐM. Phạm vi ảnh hưởng của an ninh ĐTĐM là trong vài lĩnh vực chung như: (1) An ninh và Tính riêng tư; (2) Sự tuân thủ; (3) Pháp lý hoặc Hợp đồng.

Kiến trúc của ĐTĐM gồm 3 lớp: Hạ tầng (IaaS) - Nền tảng (PaaS) - Phần mềm (SaaS) - như một dịch vụ:

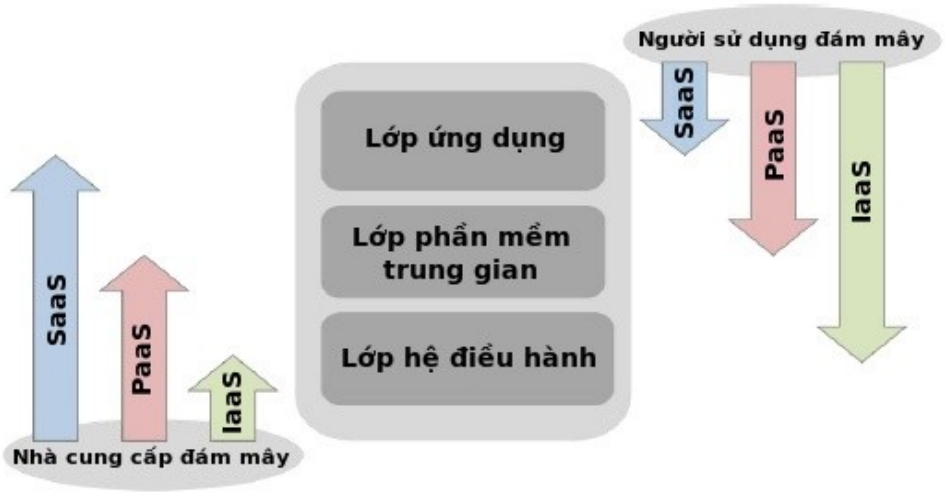
- IaaS chứa toàn bộ các tài nguyên hạ tầng trang thiết bị và phần cứng, các tài nguyên ảo hóa (nếu có), phân phối các kết nối vật lý và logic cho các tài nguyên này, cung cấp một tập hợp các APIs cho phép quản lý và tạo nên sự tương tác với hạ tầng của người sử dụng. Nó là nền tảng của tất cả các dịch vụ ĐM, PaaS và SaaS được xây lần lượt trên nó, thừa hưởng mọi rủi ro an ninh của nó.
- PaaS, so với IaaS, bổ sung thêm lớp tích hợp để xây dựng các ứng dụng trên nền tảng có sẵn: PM trung gian, ngôn ngữ & công cụ lập trình.
- SaaS đưa ra môi trường điều hành để phân phối cho người sử dụng nội dung, cách trình bày, các ứng dụng và khả năng quản lý.

Ngoài vấn đề về kiến trúc ra, một loạt các lĩnh vực khác mà các bên tham gia phải quan tâm như:

- 5 lĩnh vực về quản lý và những chỉ dẫn thực hiện: (1) Quản lý rủi ro của doanh nghiệp và chính phủ; (2) Quản lý liên quan tới việc để lộ về điện tử và pháp lý; (3) Quản lý sự tuân thủ và kiểm toán; (4) Quản lý vòng đời thông tin, dữ liệu từ khi tạo cho tới khi xóa; (5) Tính khả chuyển và tính tương hợp mà chỉ có thể giải quyết được bằng các chuẩn mở;
- 7 lĩnh vực hoạt động và những chỉ dẫn thực hiện: (1) An ninh truyền thống, tính liên tục, phục hồi thảm họa; (2) Vận hành trung tâm dữ liệu; (3) Phản ứng, thông báo, xử lý tình huống; (4) An ninh ứng dụng; (5) Mã hóa và quản lý khóa; (6) Nhận dạng và quản lý truy cập; (7) Ảo hóa.

Người sử dụng phải luôn đánh giá các rủi ro có thể khi đưa dữ liệu, ứng dụng - chức năng - qui trình ra bên ngoài và đặt ra các câu hỏi dạng như: Nếu có sự cố mất hoặc lộ thông tin - dữ liệu thì ai chịu trách nhiệm bồi thường và như thế nào? hoặc Nếu kết thúc hợp đồng thì việc chuyển các dữ liệu hoặc ứng dụng trở về với người sử dụng hoặc chuyển sang nhà cung cấp đám mây khác như thế nào?
Hiểu khái quát về kiến trúc, cùng với 12 lĩnh vực trọng tâm sống còn, sẽ cung cấp một nền tảng vững chắc cho việc đánh giá, vận hành, quản lý và chế ngự an ninh trong các môi trường ĐTĐM.
Áp dụng chuẩn ISO/IEC 27036. Các chỉ dẫn về an ninh thuê ngoài làm (dự thảo).

An toàn an ninh trong ĐTĐM có sự phân chia trách nhiệm giữa người sử dụng và nhà cung cấp dịch vụ. Với SaaS thì nhà cung cấp kiểm soát hầu như mọi thứ, trong khi với IaaS thì trách nhiệm lớn về kiểm soát an toàn an ninh thuộc về người sử dụng.



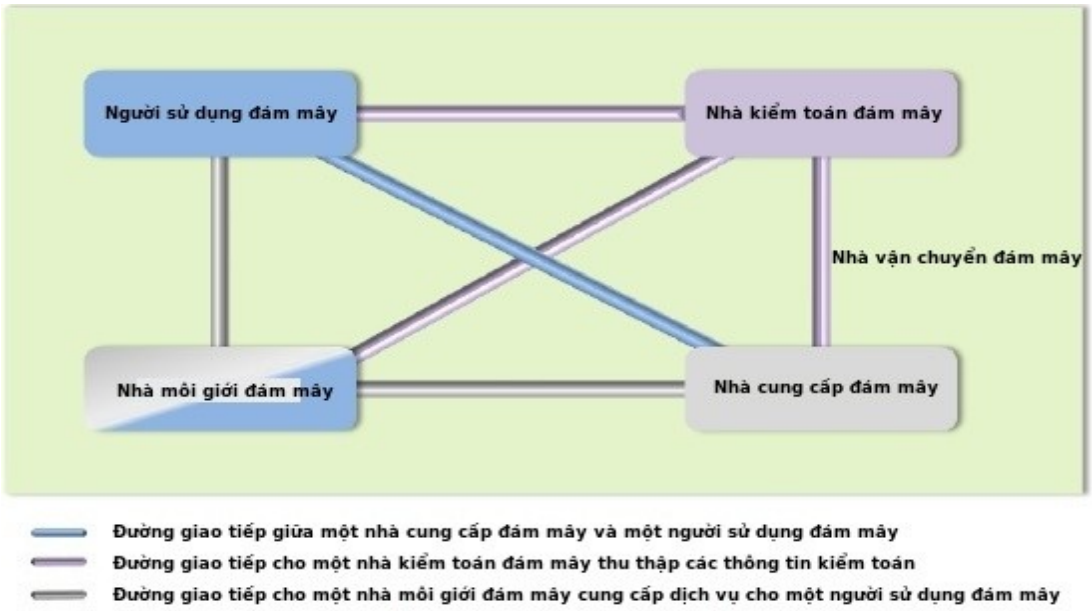
Phạm vi kiểm soát được phân chia giữa nhà cung cấp và người sử dụng

Mô hình tham chiếu khái niệm kết hợp: sơ đồ tích hợp của các thành phần hệ thống, tổ chức và qui trình trong ĐTĐM

Nhiều tác nhân tham gia trong ĐTĐM. Vì vậy rất cần xem xét tới mối quan hệ của người sử dụng với các bên liên quan.

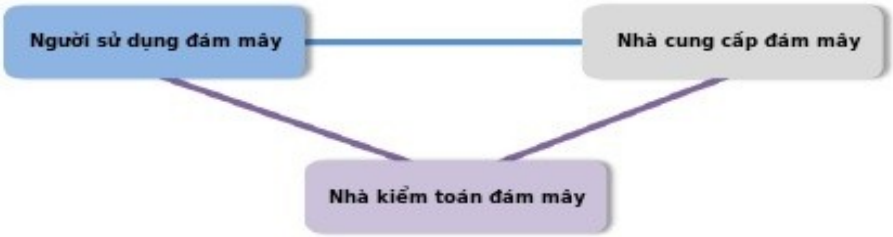
Tác nhân	Định nghĩa
Người sử dụng đám mây	Một người hoặc tổ chức duy trì một mối quan hệ nghiệp vụ với, và sử dụng dịch vụ từ, các nhà cung cấp đám mây.
Nhà cung cấp đám mây	Một người, tổ chức hoặc thực thể có trách nhiệm làm cho một dịch vụ sẵn sàng cho các bên có quan tâm.
Nhà kiểm toán đám mây	Một bên có thể tiến hành đánh giá độc lập về các dịch vụ đám mây, các hoạt động hệ thống thông tin, hiệu năng và an ninh của triển khai đám mây.
Nhà môi giới đám mây	Một thực thể quản lý sử dụng, hiệu năng và phân phối các dịch vụ đám mây, và thương thảo các mối quan hệ giữa các nhà cung cấp đám mây và những người sử dụng đám mây.
Nhà vận chuyển đám mây	Một người trung gian cung cấp kết nối và giao thông của các dịch vụ đám mây từ các nhà cung cấp đám mây cho những người sử dụng đám mây.

Các tương tác của người sử dụng với các tác nhân khác trong ĐTĐM tạo ra các kịch bản tương tác khác nhau, có ảnh hưởng tới an toàn an ninh các dịch vụ ĐTĐM.



An ninh chuỗi cung ứng - thuê ngoài khi có nhiều bên tham gia. Người sử dụng phải luôn đánh giá rủi ro đối với các dữ liệu của mình khi đặt lên đám mây. Người sử dụng luôn phải đặt câu hỏi: Liệu có rút được các dữ liệu của mình ra khỏi đám mây này để chuyển sang đám mây khác được không, cho dù các đám mây khác nhau của các nhà cung cấp khác nhau với các công nghệ được sử dụng khác nhau.

SLA: Thỏa thuận mức dịch vụ (Service Level Agreement).



Để có thêm thông tin về trách nhiệm của từng tác nhân khi tham gia vào ĐTĐM, xem "Kiến trúc tham chiếu Điện toán Đám mây của NIST. Những khuyến cáo của Viện Tiêu chuẩn và Công nghệ Quốc gia. Viện Tiêu chuẩn và Công nghệ Quốc gia, Mỹ - NIST". Tháng 09/2011. 35 trang. Các tác giả: Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger và Dawn Leaf.
URL: http://ubuntuone.com/0rqn2j5SyfKVKF6ZuEwYHC

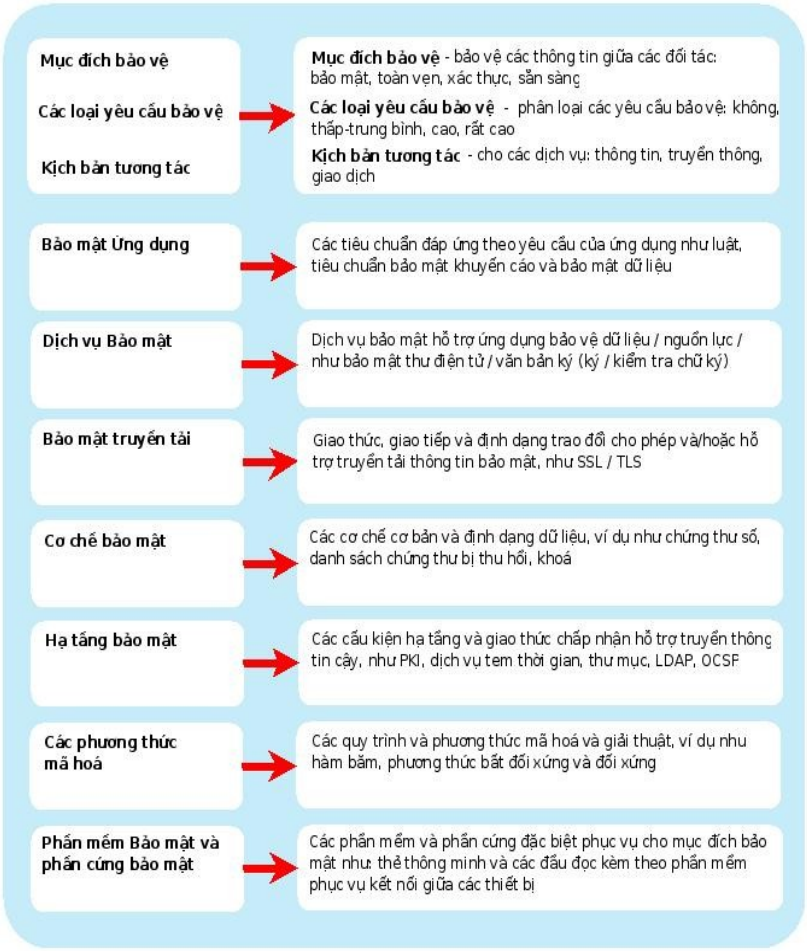
5. An ninh thông tin dữ liệu

Đảm bảo an ninh cho hạ tầng hệ thống, cho các ứng dụng... không ngoài mục tiêu cuối cùng là để đảm bảo an ninh cho thông tin dữ liệu (TTDL) và dòng luân chuyển, lưu trữ của chúng.
Một ví dụ về thành phần cơ bản an ninh dữ liệu DSC (Data Security Component) bao gồm nhiệm vụ đảm bảo an ninh cho:

1. Các giao tiếp truyền thông dựa trên web (máy trạm/máy chủ)
2. Các giao tiếp bằng thư điện tử.
3. Các chức năng về an ninh cho hệ thống phụ trợ (backend).

DSC đảm bảo các mục tiêu về an ninh sau đây:

1. Tính bí mật của TTDL, cả được truyền và được lưu trữ.
2. Tính toàn vẹn của TTDL, cả được truyền và được lưu trữ.
3. Ràng buộc tính xác thực và có thể chứng minh được.
4. Xác thực - hỗ trợ các ứng dụng dựa trên web và khác với các phương pháp xác thực khác nhau.



Mô hình cho các chuẩn an ninh thông tin dữ liệu

Trên thực tế, tùy vào mục đích bảo vệ, mức độ bảo vệ và nhiều yếu tố khác, một mô hình cho các chuẩn an ninh được thiết lập. Dựa vào mô hình này để tiến hành các cách thức bảo vệ an ninh phù hợp.

6. Chuẩn hóa như một biện pháp tăng cường an ninh thông tin dữ liệu

Việc chuẩn hóa được tiến hành theo tất cả các lớp kiến trúc của hệ thống thông tin.

1. Lớp nghiệp vụ: Chuẩn hóa qui trình nghiệp vụ, chuẩn hóa các thủ tục hành chính thông qua việc mô hình hóa chúng bằng các công cụ tiêu chuẩn UML (Unified Modeling Language).
2. Lớp thông tin: Mô hình hóa dữ liệu và chuẩn hóa dữ liệu.
   a) Có 2 mô hình dữ liệu: mô hình dữ liệu chung (được sử dụng lại trong nhiều lĩnh vực ứng dụng khác nhau) và mô hình dữ liệu đặc thù (thường được sử dụng chỉ trong một lĩnh vực),

sử dụng UML để mô hình hóa dữ liệu.

b) Tính tương hợp bao gồm tính tương hợp về tổ chức, về kỹ thuật và về ngữ nghĩa. Chuẩn hóa dữ liệu để đạt được tính tương hợp. Sử dụng ngôn ngữ đánh dấu siêu văn bản mở rộng XML (Extensible Markup Language) để chuẩn hóa việc trao đổi và sử dụng các dữ liệu trao đổi đó. Chuẩn hóa các mô hình dữ liệu đặc thù phải là ưu tiên trong chính phủ điện tử (CPĐT). Tuy vậy, việc sử dụng XML để làm chuẩn cho việc trao đổi dữ liệu là không đủ để đảm bảo cho tính tương hợp, nhất là tính tương hợp về tổ chức. Tính tương hợp về tổ chức trước tiên xác định khi nào và vì sao các dữ liệu nào đó được trao đổi. Trong tính tương hợp về tổ chức, các qui trình là kết quả của việc trao đổi các dữ liệu được phối hợp cùng với khung pháp lý tham chiếu (như việc xây dựng luật và các qui định).

3. Lớp hạ tầng: Đảm bảo cho dòng thông tin chuyển động trong hệ thống được an toàn và thông suốt. Hạ tầng mạng máy tính được thiết kế theo các vùng và việc quản lý an ninh truy cập giữa các vùng được đặt lên hàng đầu. Nhiều phần chuẩn hóa về an ninh được thực hiện cho lớp này.
4. Lớp ứng dụng: Các module thành phần, các ứng dụng - dịch vụ dùng chung, kiến trúc phần mềm tham chiếu như các mô hình kiến trúc thành phần, SOA, SaaS, "điện toán đám mây"... 4Ứng với mỗi mô hình kiến trúc, sẽ có những khác biệt nhất định đặc trưng cho kiến trúc đó.
   a) Việc chuẩn hóa ở đây có thể liên quan tới hầu hết các lĩnh vực được thể hiện trong một GIF (Government Interoperability Framework), thường được chia thành các lĩnh vực như: (1) kết nối nội bộ, (2) tích hợp dữ liệu, (3) truy cập dữ liệu và trình diễn, (4) an ninh, (5) các dịch vụ web, (6) siêu dữ liệu, có thể có thêm (7) khu vực các nghiệp vụ...
   b) Việc chuẩn hóa cũng có thể được thực hiện thông qua việc kết hợp với kiến trúc tổng thể thường thấy trong các NEA (National Enterprise Architecture). Theo cách này thì các chuẩn được phân loại theo các kiến trúc phân tầng.
5. Lớp công nghệ: Chuẩn cho các loại công nghệ - mô hình kiến trúc phần mềm tham chiếu được lựa chọn (thành phần, SOA, SaaS, "đám mây"...) nhằm đảm bảo cho tính tương hợp, tính sử dụng lại được, tính mở, an ninh, mở rộng theo phạm vi, tính riêng tư, hỗ trợ thị trường... Đưa ra bộ chuẩn lựa chọn theo vòng đời của chuẩn cho:
   a) Kiến trúc ứng dụng, dịch vụ có và không có phần mềm trung gian
   b) Phần mềm máy trạm - truy cập thông tin dựa trên web/máy tính/điện thoại di động/PDA/từ các hệ thống bên ngoài
   c) Việc trình diễn, xử lý thông tin đối với các loại thiết bị nêu trên.
   d) Giao tiếp: chọn các giao thức cho phần mềm trung gian, mạng, ứng dụng, dịch vụ thư mục, dịch vụ địa lý.
   e) Kết nối tới backend.
   f) Các chuẩn về an ninh dữ liệu - mô hình cho các chuẩn an ninh thông tin dữ liệu.

Vòng đời của các chuẩn thường được sử dụng để các chuẩn được liên tục cập nhật theo sự tiến hóa của công nghệ và hiện trạng nền CNTT-TT của nơi áp dụng. Vì vậy các chuẩn thường được phân loại theo các tình trạng dạng như: "bắt buộc sử dụng", "khuyến cáo sử dụng" và "đang được theo dõi".

7. Chuẩn mở là một biện pháp đảm bảo an ninh thông tin dữ liệu

1. Định nghĩa chuẩn mở: Có nhiều định nghĩa khác nhau về chuẩn mở. Tuy nhiên có một số điểm chung như sau:
   a) Tiêu chuẩn được áp dụng và được một tổ chức phi lợi nhuận duy trì, và sự phát triển hiện

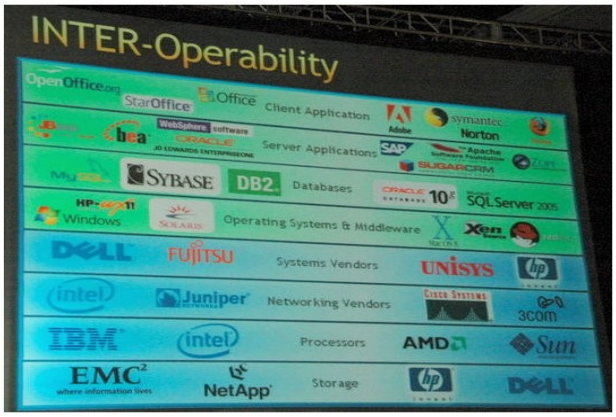
hành của nó diễn ra trên cơ sở của một thủ tục ra quyết định mở, sẵn sàng cho tất cả các bên có quan tâm (quyết định đồng thuận hoặc theo số đông...).

b) Tiêu chuẩn đã được xuất bản và tài liệu đặc tả của chuẩn là sẵn sàng hoặc một cách tự do hoặc với một phí tượng trưng. Tất cả mọi người phải được phép sao chép, phân phối và sử dụng nó mà không mất phí hoặc với một phí tượng trưng.

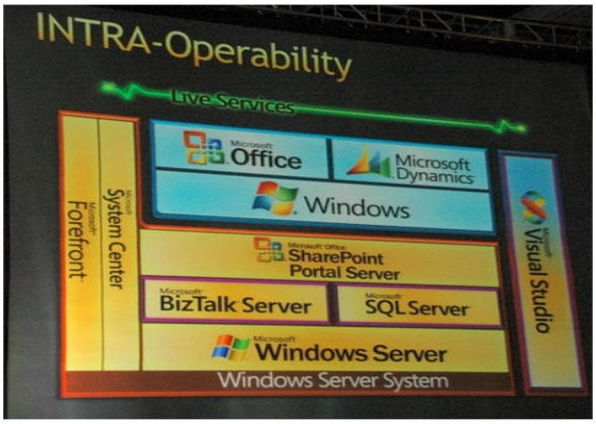
c) Sở hữu trí tuệ - nghĩa là, các bằng sáng chế có thể là có - đối với (các phần) tiêu chuẩn và được làm cho sẵn sàng không thể hủy bỏ được trên cơ sở không có phí bản quyền.

d) Không có bất kỳ ràng buộc nào trong việc sử dụng lại tiêu chuẩn đó.

2. Vì sao an ninh được đảm bảo tốt hơn khi sử dụng các chuẩn mở?
   a) Không bị khóa trói vào nhà cung cấp đặc biệt nào
   b) Bảo toàn TTDL cho lâu dài
   c) Đảm bảo tính tương hợp liên thông của TTDL trong các hệ thống
   d) Dễ dàng chuyển TTDL từ hệ thống này sang hệ thống khác
   e) Khuyến khích đổi mới sáng tạo, tăng sức cạnh tranh, làm hạ giá thành sản phẩm...
3. Tính tương hợp (tính tương thích liên thông) là yếu tố sống còn cho CPĐT
   a) Định nghĩa: Tính tương hợp, ở nghĩa rộng, là khả năng các bên tham gia làm việc được với nhau. Về khía cạnh kỹ thuật, đây là khả năng của 2 hoặc nhiều hệ thống hoặc thành phần CNTT-TT trao đổi thông tin và sử dụng các thông tin được trao đổi đó nhằm mục đích cải thiện việc điều hành và quản lý của chính phủ. Vì đặc điểm về tổ chức của một chính phủ luôn được tạo nên từ nhiều bộ, ngành, tỉnh mà tại mỗi nơi này đều có những hệ thống thông tin của mình nên tính tương hợp là một trong những yếu tố quan trọng mang tính sống còn trong việc xây dựng CPĐT.



Tính tương hợp thực sự – Interoperability
Chúng ta nên theo - sân chơi cho mọi người



Tính tương hợp cục bộ – Intraoperability
Chúng ta nên tránh - Khóa trói vào nhà cung cấp

   b) Tồn tại tính tương hợp về tổ chức, công nghệ và ngữ nghĩa.
   c) Trong thực tế, tồn tại 2 khái niệm: tính tương hợp cục bộ và tính tương hợp thực sự.
   d) Chuẩn mở là yếu tố quan trọng trong bất kỳ khung tương hợp GIF nào. Chuẩn mở là xương sống của một tiếp cận dựa trên dịch vụ cho tính tương hợp CPĐT.
4. Ví dụ nổi bật về chuẩn mở chính là giao thức TCP/IP của Internet, có xuất xứ tử mạng ARPANET của Bộ quốc phòng Mỹ.

8. Mô hình độ chín an ninh không gian mạng

Một trong những mô hình được sử dụng phổ biến hiện nay để đánh giá tiềm lực tấn công và phòng thủ về an ninh không gian mạng (ANKGM) và chiến tranh không gian mạng (CTKGM) của các quốc gia trên thế giới là mô hình độ chín ANKGM.

8.1. Đặc điểm của các phần mềm độc hại cao cấp ngày nay

Ngày nay, bức tranh của các mối đe dọa ANKGM đã khác so với trước kia, đã có một dòng mới các cuộc TCKGM là cao cấp, có đích ngắm và dựa vào các lỗi ngày số 0 của các phần mềm. Có thể mô tả đặc điểm của các phần mềm độc hại ngày nay so với trước kia như sau:

Về mức độ giấu giếm: Từ các phần mềm độc hại được biết một cách công khai tiến tới các phần mềm độc hại được giấu giếm cao độ và thường được che giấu ngụy trang khéo léo.

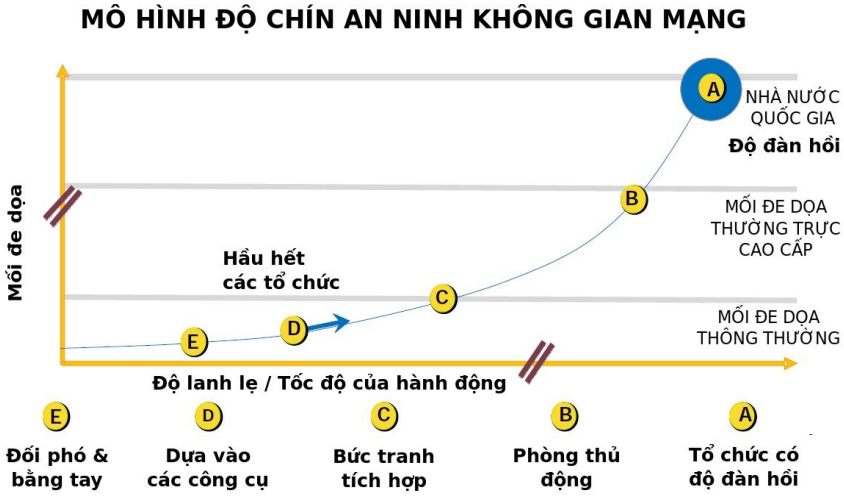
Về mức độ nhận biết: Từ các phần mềm độc hại nhằm vào những chỗ bị tổn thương có thể nhận biết được mà chưa được vá tiến tới các phần mềm độc hại nhằm vào những chỗ bị tổn thương chưa từng được biết, những lỗi ngày số 0, những lỗi phần mềm chưa từng được vá trước đó.

Về mức độ rộng rãi: Từ các phần mềm độc hại có mục đích chung một cách rộng rãi với các nạn nhân là những người vô tình bị rơi vào bẫy tiến tới các phần mềm độc hại có đích ngắm cụ thể, vào một phần mềm cụ thể, thậm chí của một hãng sản xuất cụ thể với "những nạn nhân cần quan tâm đặc biệt".

Về mức độ thường trực: Từ các phần mềm độc hại được tạo ra để gây tác hại một lần tiến tới các phần mềm độc hại tác động thường trực liên tục với mã nguồn của phần mềm độc hại được cập nhật và duy trì liên tục để gây ra sự dừng hoạt động dài hạn của cả hệ thống.

8.2. Mô hình độ chín ANKGM

Mô hình độ chín ANKGM với 5 giai đoạn hướng tới sự đàn hồi chống lại các cuộc TCKGM trải từ các mối đe dọa thông thường tới mối đe dọa thường trực cao cấp, trải từ việc hành động đối phó bằng tay trước các cuộc TCKGM cho tới việc đảm bảo độ đàn hồi của toàn bộ hệ thống.



Giải nghĩa các mức độ đối phó với các cuộc TCKGM

E. Mọi người dựa vào việc tuân theo

học thuyết và làm cách tốt nhất họ có thể để "dập tắt lửa".
D. Áp dụng từng phần các công cụ và công nghệ để hỗ trợ mọi người đối phó được nhanh hơn với các cuộc TCKGM.
C. Hệ thống được tích hợp với trọng tâm hướng vào tính tương hợp và các tiêu chuẩn trao đổi dữ liệu về nhận thức tình huống bảo an thông tin.
B. Lanh lẹ và dự đoán trước được các tình huống liên quan tới ANKGM và các cuộc TCKGM, đưa ra chính sách nhanh chóng và chuyên nghiệp, làm sáng tỏ các sự kiện và giúp những người vận hành tìm, sửa và nhằm vào việc đối phó lại.
A. Dự đoán trước được các tình huống và tập trung vào nhiệm vụ, cô lập được và chịu đựng được thiệt hại nếu có, đảm bảo an ninh cho các chuỗi cung ứng và bảo vệ các hạ tầng sống còn chủ chốt để vận hành qua được các cuộc TCKGM.

Xếp hạng theo mô hình độ chín ANKGM của 23 quốc gia được khảo sát tháng 0-2/2012

Điểm tối đa là 5	Quốc gia	Học thuyết/ Chiến lược ANKGM	Có CERT* quốc gia	Tham gia cộng động CERT*	Chỉ huy ANKGM quốc gia	Diễn tập ANKGM
4.5/5	Phần Lan		Có	Có		Có
	Israel	Có	Có	Có	Có	
	Thụy Điển	Có	Có	Có		Có
4.0/5	Đan Mạch		Có	Có		
	Estonia	Có - 2008	Có	Có		Có
	Pháp	Có - 2011	Có	Có		Có
	Đức	Có - 2011	Có	Có		Có
	Hà Lan	Có - 2011	Có	Có		Có
	Tây Ban Nha		Có	Có	Có	
	Anh	Có - 2011	Có	Có	Có	Có
	Mỹ	Có - 2011	Có	Có	Có	Có
3.5/5	Úc	Có - 2009			Có	
	Áo		Có	Có		
	Canada	Có	Có	Có		
	Nhật	Có	Có	Có	Có	
3.0/5	Trung Quốc	Có	Có	Có		
	Ý		Có			Có
	Balan		Có	Có		Có
	Nga	Có	Có	Có	Có	

Điểm tối đa là 5	Quốc gia	Học thuyết/ Chiến lược ANKGM	Có CERT* quốc gia	Tham gia cộng động CERT*	Chỉ huy ANKGM quốc gia	Diễn tập ANKGM
2.5/5	Brazil	Có	Có	Có	Có	
	Ấn Độ		Có			
	Rumani	Có	Có	Có		
2.0/5	Mexico					

* CERT: Đội ứng cứu khẩn cấp sự cố máy tính.

8.3. Lưu ý quan trọng từ mô hình độ chín ANKGM

Trong mức C của mô hình độ chín ANKGM nhấn mạnh tới tính tương hợp của hệ thống thông tin và các tiêu chuẩn trao đổi dữ liệu về nhận thức tình huống bảo an thông tin. Điều này gợi ý rằng:

1. Để có được những thông tin kịp thời, chính xác nhằm đối phó với sự việc mất an ninh theo một cách thống nhất giữa tất cả các bên tham gia trong việc đảm bảo an toàn an ninh các hệ thống thông tin, thì tính tương hợp và các tiêu chuẩn dựa vào sự trao đổi dữ liệu về nhận thức tình huống bảo an thông tin là một yếu tố sống còn.
2. Việc không đạt được tính tương hợp dựa vào các tiêu chuẩn trao đổi dữ liệu về nhận thức tình huống bảo an thông tin ở mức C thì sẽ không thể tiến tới các mức cao hơn B và A trong mô hình độ chín ANKGM được. Nói cách khác, nếu không đạt được tính tương hợp thì hệ thống thông tin không bao giờ đạt được mức C trong mô hình độ chín ANKGM được.
3. Khi xây dựng các hệ thống thông tin hướng tới CPĐT, nên kết hợp với mô hình độ chín ANKGM, đặc biệt đối với các bên có trách nhiệm tham gia trong việc đảm bảo an toàn an ninh các hệ thống thông tin, để vừa đạt được các mục tiêu về giải quyết các vấn đề nghiệp vụ cũng như các mục tiêu về an ninh của toàn bộ hệ thống thông qua việc đảm bảo tính tương hợp cho các thông tin - dữ liệu dựa vào các tiêu chuẩn mở.

Xem thêm: Giới thiệu sơ lược mô hình độ chín an ninh không gian mạng để có chi tiết hơn về mô hình độ chín ANKGM

9. Nguồn của các mối đe dọa và dạng các lỗ hổng thường gặp về an ninh

Các nguồn của các mối đe dọa an ninh không gian mạng và các dạng khai thác có liên quan tới an ninh không gian mạng thường gặp hiện nay.

Các dạng khác nhau của những mối đe dọa từ nhiều nguồn có thể ảnh hưởng bất lợi cho:

- Các máy tính, phần mềm, mạng,
- Các hoạt động của một cơ quan, một nền công nghiệp, hoặc bản thân Internet.

Các mối đe dọa không gian mạng có thể là vô tình hoặc cố ý.

- Các mối đe dọa do vô tình có thể gây ra bằng việc nâng cấp phần mềm hoặc duy trì các thủ tục mà chúng gây ngắt quãng một cách vô tình cho các hệ thống.
- Các mối đe dọa cố ý gồm cả các cuộc tấn công có chủ đích và không có chủ đích. Các cuộc tấn công có thể tới từ một loạt các nguồn, bao gồm các nhóm tội phạm, các tin tặc, và các tên

khủng bố...

9.1. Tác nhân của các mối đe dọa về an ninh không gian mạng

Mối đe dọa	Mô tả
Những người vận hành các botnet	Những người vận hành các botnet sử dụng một mạng – botnet của các máy tính bị tổn thương, bị kiểm soát từ xa để phân phối các cuộc tấn công theo kế hoạch bằng phishing, spam, và phần mềm độc hại. Các dịch vụ của các mạng này đôi khi được làm sẵn trên các thị trường ngầm (như, việc mua sắm một cuộc tấn công từ chối dịch vụ hoặc các máy chủ để sắp đặt các cuộc tấn công bằng spam hoặc phishing).
Các nhóm tội phạm	Các nhóm tội phạm tìm các hệ thống để tấn công và lấy tiền. Đặc biệt, các nhóm tội phạm có tổ chức sử dụng spam, phishing, và phần mềm gián điệp/phần mềm độc hại để phạm tội ăn trộm nhận dạng và giả mạo trực tuyến. Bọn gián điệp của các tổ chức quốc tế và các tổ chức tội phạm có tổ chức cũng đặt ra mối đe dọa cho quốc gia thông qua khả năng của chúng tiến hành gián điệp công nghiệp và phạm tội ăn trộm ở phạm vi lớn và thuê hoặc phát triển các tài năng tin tặc.
Các tin tặc	Các tin tặc đột nhập vào các mạng với mục đích như làm rung động thách thức, khoe khoang các quyền trong cộng đồng tin tặc, trả thù, lén săn đuổi những người khác, lấy tiền và những lý do khác. Trong khi để giành được sự truy cập không được phép từng đòi hỏi một số lượng khá các kỹ năng hoặc tri thức về máy tính, thì các tin tặc bây giờ tải các script và các giao thức tấn công về từ Internet và tung chúng ra chống lại các site nạn nhân. Vì thế, khi các công cụ tấn công đã trở nên tinh vi phức tạp hơn, thì chúng cũng trở nên dễ dàng sử dụng hơn. Theo Cục Tình báo Trung ương Mỹ – CIA, đa số lớn các tin tặc không có được sự tinh thông cần thiết để đe dọa các mục tiêu khó khăn như các mạng sống còn của quốc gia. Tuy nhiên, số lượng các tin tặc trên thế giới đặt ra một mối đe dọa khá cao đối với một sự đổ vỡ ngắn hạn và bị cách ly gây ra tổn thất nghiêm trọng.
Người bên trong	Người bên trong tổ chức bất mãn là một nguồn cơ bản của tội phạm máy tính. Những người bên trong có thể không cần nhiều hiểu biết về những thâm nhập trái phép của máy tính vì hiểu biết của họ về một hệ thống đích thường cho phép họ giành được sự truy cập không giới hạn để gây thiệt hại cho hệ thống hoặc ăn cắp các dữ liệu hệ thống. Mối đe dọa của người bên trong cũng bao gồm các nhà thầu được tổ chức thuê, cũng như các nhân viên mà ngẫu nhiên đưa phần mềm độc hại vào trong hệ thống.
Các quốc gia	Các quốc gia sử dụng các công cụ không gian mạng như một phần của các hoạt động thu thập và gián điệp thông tin và/hoặc phá hoại của họ. Một số quốc gia đang làm việc tích cực để phát triển học thuyết, các chương trình và các khả năng của chiến tranh thông tin. Những khả năng như vậy cho phép một thực thể đơn nhất có được tác động đáng kể và nghiêm túc bằng việc phá hoại các hạ tầng cung ứng, truyền thông và kinh tế mà chúng hỗ trợ cho sức mạnh quân sự – những tác động mà có thể ảnh hưởng cho những cuộc sống hàng ngày của các công dân trên khắp đất nước. Các sâu đặc biệt nguy hiểm do nhà nước tài trợ như Stuxnet, Duqu, Flame... không chỉ có chức năng

Mối đe dọa	Mô tả
	gián điệp thông tin, mà còn phá hoại các cơ sở hạ tầng sống còn của một quốc gia.
Những người đánh phishing	Các cá nhân, hoặc các nhóm nhỏ, thực hiện các kế hoạch phishing với mong muốn ăn cắp các nhận dạng hoặc thông tin để lấy tiền. Những người đánh phishing cũng có thể sử dụng spam và các phần mềm gián điệp/phần mềm độc hại để hoàn thành các mục tiêu của họ.
Những người đánh spam	Các cá nhân hoặc các tổ chức phân phối thư điện tử không theo yêu cầu với những thông tin ẩn hoặc sai để bán các sản phẩm, tiến hành các kế hoạch phishing, phân phối các phần mềm gián điệp/phần mềm độc hại, hoặc tấn công các tổ chức (như, tấn công từ chối dịch vụ).
Các tác giả của phần mềm gián điệp/phần mềm độc hại	Các cá nhân hoặc tổ chức với dự định độc hại triển khai các cuộc tấn công chống lại những người sử dụng bằng việc sản xuất và phân phối các phần mềm gián điệp và phần mềm độc hại. Một số virus và sâu máy tính có tính phá hoại đã làm hỏng các tệp và các ổ đĩa cứng, bao gồm cả Melissa Macro Virus, sâu Explore.Zip, CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, và Blaster...
Những kẻ khủng bố	Những kẻ khủng bố tìm để phá hủy, vô hiệu hóa, hoặc khai thác các hạ tầng sống còn để đe dọa an ninh quốc gia, gây ra những thiệt hại hàng loạt, làm yếu đi nền kinh tế, và gây thiệt hại về đạo đức và sự tin cậy vào nhà nước. Những kẻ khủng bố có thể sử dụng các kế hoạch phishing hoặc phần mềm gián điệp/phần mềm độc hại để làm tiền hoặc thu thập những thông tin nhạy cảm.
Các nguồn: Các phân tích của Văn phòng Kiểm toán Liên bang Mỹ (GAO) trên các dữ liệu từ Giám đốc Tình báo Quốc gia, Bộ Tư pháp, Văn phòng Điều tra Liên bang Mỹ FBI, Cơ quan Tình báo Trung ương Mỹ CIA, và Trung tâm Điều phối CERT của Viện Kỹ thuật Phần mềm.	

Các dạng khác nhau về các mối đe dọa không gian mạng có thể sử dụng một loạt các khai thác không gian mạng có khả năng ảnh hưởng bất lợi cho các máy tính, phần mềm, mạng, các hoạt động của cơ quan, của nền công nghiệp, hoặc của bản thân Internet (xem Bảng bên dưới). Các nhóm hoặc các cá nhân có thể triển khai một cách có chủ ý những khai thác không gian mạng nhằm vào một tài sản không gian mạng cụ thể nào đó hoặc tấn công thông qua Internet có sử dụng virus, sâu, hoặc phần mềm độc hại mà không có mục tiêu cụ thể nào.

9.2. Một số dạng khai thác lỗ hổng an ninh không gian mạng thường gặp

Dạng khai thác	Mô tả
Từ chối dịch vụ	Một phương pháp tấn công từ một nguồn đơn nhất mà từ chối sự truy cập hệ thống đối với những người sử dụng hợp pháp bằng việc gây tràn ngập máy tính đích với các thông điệp và cản trở giao thông hợp pháp. Nó có thể ngăn cản một hệ thống để nó không có khả năng trao đổi các dữ liệu với các hệ thống khác hoặc sử dụng Internet.
Từ chối	Một biến thể của tấn công từ chối dịch vụ có sử dụng một cuộc tấn công được phối hợp

Dạng khai thác	Mô tả
dịch vụ phân tán	từ một hệ thống các máy tính phân tán hơn là từ một nguồn đơn nhất. Nó thường sử dụng các sâu để lan truyền ra nhiều máy tính để các máy tính này sau đó tấn công mục tiêu.
Công cụ khai thác	Các công cụ có sẵn một cách công khai và tinh vi phức tạp mà những kẻ thâm nhập trái phép với các mức độ về kỹ năng khác nhau có thể sử dụng để xác định những chỗ bị tổn thương và thâm nhập vào các hệ thống mục tiêu.
Bom Logic	Một dạng phá hoại trong đó một lập trình viên chèn mã và mã này làm cho chương trình thực thi một hành động phá hoại khi một số sự kiện kích hoạt xảy ra, như việc kết thúc việc làm của lập trình viên.
Phishing	Việc tạo và sử dụng các thư điện tử và các website – được thiết kế để trông giống như các doanh nghiệp, các cơ quan tài chính và các cơ quan chính phủ hợp pháp nổi tiếng – để lừa dối những người sử dụng Internet phơi các dữ liệu cá nhân của họ ra, như các thông tin và các mật khẩu tài khoản tài chính và ngân hàng. Những kẻ đánh phishing sau đó sử dụng các thông tin này cho những mục đích tội phạm, như ăn trộm và lừa gạt.
Kẻ hít gói (Sniffer)	Đồng nghĩa với kẻ hít các gói. Một chương trình chặn các dữ liệu được định tuyến và kiểm tra từng gói để tìm các thông tin đặc biệt, như các mật khẩu được truyền ở dạng các văn bản rõ ràng.
Ngựa Trojan	Một chương trình máy tính giấu mã độc hại. Một ngựa Trojan thường ngụy trang như một chương trình hữu dụng mà người sử dụng có thể mong muốn để chạy.
Virus	Một chương trình lây nhiễm cho các tệp máy tính, thường là các chương trình có thể chạy được, bằng việc chèn một bản sao của chính nó vào tệp đó. Các bản sao thường chạy được khi tệp bị lây nhiễm được tải vào bộ nhớ, cho phép virus lây nhiễm các tệp khác. Không giống như một sâu máy tính, một virus đòi hỏi sự liên quan của con người (thường không có chủ tâm) để nhân giống.
Vishing	Phương pháp của phishing dựa trên công nghệ của giao thức tiếng nói qua Internet (VoIP) và phần mềm của trung tâm gọi nguồn mở mà đã làm cho nó thành không đắt giá cho những kẻ mưu đồ bất lương để thiết lập các trung tâm gọi điện thoại và bọn tội phạm gửi đi các thông điệp thư điện tử và văn bản tới các nạn nhân tiềm năng, nói đã có một vấn đề về an ninh, và họ cần gọi cho ngân hàng của họ để kích hoạt lại một thẻ tín dụng hoặc thẻ nợ, hoặc gửi các thông điệp văn bản tới các máy tính cầm tay, ra lệnh cho những nạn nhân tiềm năng để liên hệ với các ngân hàng trực tuyến giả mạo để thay mới lại các tài khoản của họ.
Lái chiến tranh (War driving)	Phương pháp thâm nhập vào các mạng máy tính không dây bằng việc sử dụng một máy tính xách tay, ăng ten, và bộ adapter của mạng không dây liên quan tới việc tuần tra các vị trí để giành được sự thâm nhập trái phép.
Sâu (Worm)	Một chương trình máy tính độc lập mà nó tái sinh bằng việc tự sao chép nó từ hệ thống này sang hệ thống khác qua mạng. Không giống như những virus máy tính, các sâu không đòi hỏi sự liên quan của con người để nhân giống.

Dạng khai thác	Mô tả
Khai thác ngày số 0 (Zero-day)	Mối đe dọa không gian mạng tận dụng một chỗ bị tổn thương về an ninh trong cùng ngày mà chỗ bị tổn thương đó được biết đối với công chúng nói chung và đối với nó thì còn chưa có bản sửa lỗi nào có sẵn.
Các nguồn: Các phân tích dữ liệu của Văn phòng Kiểm toán Liên bang Mỹ (GAO) và từ các báo cáo của giới công nghiệp.	

9.3. Những vấn đề liên quan khác tới an ninh

- Mối đe dọa về an ninh xuất phát từ chuỗi cung ứng sản phẩm - giải pháp, cả phần cứng, phần mềm và các thiết bị viễn thông - những thành phần không thể thiếu của hệ thống thông tin cũng đang nổi lên như một chủ đề nóng hiện nay tại một số quốc gia trên thế giới.
- Luật Yêu nước của Mỹ: Luật Yêu nước của Mỹ yêu cầu một công ty Mỹ (hoặc các chi nhánh của nó) phải truyền tay gần như tất cả các dữ liệu công ty có về người sử dụng theo yêu cầu của các cơ quan an ninh Mỹ như FBI, mà không cần lệnh của tòa án.

10. Các công cụ an ninh

10.1. Danh sách 65 sự thay thế của nguồn mở cho các phần mềm an ninh

Các ứng dụng nguồn mở có khả năng thay thế các ứng dụng nguồn đóng cho việc chống virus, chống spam, làm tường lửa, mã hóa và các vấn đề khác có liên quan tới an ninh các hệ thống thông tin.

Loại	Tên phần mềm	Thay thế cho	Mô tả
Chống Spam	ASSP	Barracuda Spam and Virus Firewall, SpamHero, Abaca Email Protection Gateway	Tự giới thiệu như là "vũ khí chống SPAM tốt nhất tuyệt đối mà thế giới biết từ trước tới này", ASSP nằm trong các máy chủ SMTP của bạn để dừng các spam và quét virus. Các tính năng bao gồm thiết lập dựa vào trình duyệt, hỗ trợ cho hầu hết các máy chủ SMTP, các danh sách trắng tự động, kiểm tra hợp lệ người gửi sớm, lọc Bayesian và nhiều hơn thế. Hệ điều hành: Không phụ thuộc OS.
	MailScanner	Barracuda Spam and Virus Firewall, SpamHero, Abaca Email Protection Gateway	Được tải về hơn 1.3 triệu lần từ những người sử dụng tại 225 quốc gia, MailScanner là một gói an ninh thư điện tử tự do cho các máy chủ thư điện tử. Nó kết hợp với SpamAssassin, ClamAV và một số công cụ khác để khóa spam và phần mềm độc hại. Hệ điều hành: Độc lập với OS.
	SpamAssassin	Barracuda Spam	"Bộ lọc spam nguồn mở mạnh số 1", SpamAssasin sử

Loại	Tên phần mềm	Thay thế cho	Mô tả
		and Virus Firewall, SpamHero, Abaca Email Protection Gateway	dụng phân tích văn bản và đầu đề, lọc Bayesian, các danh sách khóa DNS, các cơ sở dữ liệu lọc cộng tác và các kỹ thuật khác để khóa spam. Dự án này được Quỹ Apache quản lý, và được kết hợp vào một số sản phẩm nguồn mở và thương mại khác. Hệ điều hành: ban đầu là Linux và OS X, dù các phiên bản cho Windows vẫn có.
	SpamBayes	Barracuda Spam and Virus Firewall, SpamHero, Abaca Email Protection Gateway	Như bạn có thể đoán từ cái tên, dự án này đưa ra một nhóm các bộ lọc Bayesian cho việc khóa spam. Site này bao gồm các phiên bản cho Outlook, Outlook Express, Windows Live Mail, IncrediMail, Thunderbird, Gmail, Yahoo Mail và các trình thư khács. Hệ điều hành: Độc lập với OS
	Nixory	SpyBot Search and Destroy, AdAware	Nixory loại bỏ và khóa các cookies theo dõi độc hại (phần mềm gián điệp) từ máy của bạn. Nó hỗ trợ cho Mozilla Firefox, Internet Explorer và Google Chrome, và nó sẽ không làm chậm máy của bạn trong khi bạn lướt web. Hệ điều hành: Độc lập với OS.
Chống virus / chống phần mềm độc hại	ClamAV	Avast! Linux Edition, VirusScan Enterprise for Linux	Đây là máy chống virus phổ biến nhất đã được kết hợp vào trong vô số các sản phẩm an ninh và tự gọi nó là "tiêu chuẩn de facto cho việc quét các cổng gateway thư". Phiên bản nguồn mở chạy trên các máy chủ thư UNIX hoặc Linux, nhưng website cũng đưa ra một phiên bản gọi là Immunet cho các máy tính cá nhân PC Windows. Hệ điều hành: Linux.
	ClamTK	Avast! Linux Edition, VirusScan Enterprise for Linux	ClamTK làm cho ClamAV dễ dàng hơn một chút để sử dụng bằng việc cung cấp một giao diện đồ họa cho máy chống virus. Giống như bản gốc, nó chạy trên Linux và quét theo yêu cầu. Hệ điều hành: Linux.
	ClamWin Free Antivirus	Kaspersky Anti-Virus, McAfee AntiVirus Plus, Norton Anti-Virus	Dựa vào ClamAV, ClamWin bảo vệ hơn 600.000 PC khỏi các virus và phần mềm độc hại. Lưu ý rằng không giống như hầu hết các gói chống virus thương mại, ClamWin không đưa ra một máy quét thời gian thực khi truy cập; để quét các tệp đến, bạn sẽ cần lưu chúng và sau đó chạy một lượt quét bằng tay trước khi mở hoặc chạy các tệp. Hệ điều hành: Windows.
	P3Scan	Avast! Linux Edition,	Với P3Scan, bạn có thể thiết lập một máy chủ ủy quyền proxy trong suốt mà đưa ra được sự bảo vệ chống virus

Loại	Tên phần mềm	Thay thế cho	Mô tả
		VirusScan Enterprise for Linux	và chống spam. Hệ điều hành: Linux.
Sao lưu	Amanda	Simpana Backup and Recovery, NetVault, HP StorageWorks EBS	Bảo vệ hơn 500.000 máy trên thế giới, Amanda nói là "phần mềm sao lưu và phục hồi nguồn mở phổ biến nhất trên thế giới". Bổ sung thêm vào phiên bản cộng đồng, nó cũng có sẵn hỗ trợ phiên bản doanh nghiệp hoặc là một thiết bị. Hệ điều hành: Windows, Linux, OS X.
	Areca Backup	NovaBackup	Nhằm vào cho một sự cân bằng giữa đơn giản và đa dạng, Areca đưa ra một giao diện đồ họa dễ dàng với nhiều lựa chọn cho việc tạo và tương tác với các tệp lưu trữ. Các tính năng chính bao gồm nén, mã hóa, hỗ trợ sao lưu delta, trộn lưu trữ và hơn thế nữa. Hệ điều hành: Windows, Linux.
	Bacula	Simpana Backup and Recovery, NetVault, HP StorageWorks EBS	Được thiết kế cho những người sử dụng doanh nghiệp, Bacula sao lưu nhiều hệ thống khắp một mạng. Hỗ trợ và các dịch vụ thương mại cho sản phẩm phổ biến là sẵn sàng thông qua Bacula Systems. Hệ điều hành: Windows, Linux, OS X.
	Clonezilla	Norton Ghost	Được tạo ra như một lựa chọn thay thế cho Ghost, Clonezilla có thể bắt chước các hệ thống đơn hoặc đa rất nhanh. Nó có 2 phiên bản: Clonezilla Live cho các máy đơn và Clonezilla SE cho các mạng lớn. Hệ điều hành: Windows, Linux, OS X.
	Partimage	Norton Ghost, NovaBackup, McAfee Online Backup, Carbonite.com	Partimage có thể tạo một ảnh hoàn chỉnh máy của bạn, mà là hữu dụng nếu bạn cần phục hồi từ một sự hỏng máy hoàn toàn hoặc nếu bạn muốn cấu hình cho nhiều hệ thống với chính xác các phần mềm y hệt. Nó cũng có thể tạo một phân vùng phục hồi trên đĩa của bạn. Hệ điều hành: Linux.
	Redo	Norton Ghost, NovaBackup, McAfee Online Backup, Carbonite.com	Tự gọi mình là "Giải pháp phục hồi thảm họa hoàn chính nhất, dễ nhất sẵn có", Redo đưa ra các khả năng sao lưu, phục hồi và phục hồi bare-metal. Thậm chí trong các trường hợp khẩn cấp khắc nghiệt nhất khi bạn phải thay thế một ổ cứng hoàn toàn, thì Redo nói nó có thể làm cho bạn sao lưu và chạy được với tất cả các chương trình của bạn và các tệp chỉ trong 10 phút. Hệ điều hành: Linux.
Trình	Chromium	Microsoft	Phiên bản nguồn mở của Google Chrome, Chromium có

Loại	Tên phần mềm	Thay thế cho	Mô tả
duyệt		Internet Explorer	xu hướng sẽ nhanh hơn và an ninh hơn so với các trình duyệt cạnh tranh. Các đặc tính an ninh chủ chốt bao gồm sandboxing, tự động cập nhật, SafeBrowsing và hơn thế nữa. Hệ điều hành: Windows, Linux, OS X.
	Dooble	Microsoft Internet Explorer	Các lập trình viên Dooble đã tạo ra trình duyệt mới hơn này với một sự quan tâm về an toàn và dễ sử dụng. Không giống như hầu hết các trình duyệt khác, nó tự động mã hóa tất cả các giao thông cho tính riêng tư và an ninh lớn hơn. Hệ điều hành: Windows, Linux, OS X.
	Tor	Microsoft Internet Explorer	Tor bảo vệ sự nhận diện của bạn bằng việc cung cấp tính nặc danh trong khi bạn duyệt Web. Được các phóng viên, các nhà hoạt động xã hội và những người khác sử dụng với quan tâm rằng ai đó có thể ăn cắp trong các hoạt động trực tuyến của họ. Hệ điều hành: Windows, Linux, OS X.
Bổ sung của trình duyệt	Web of Trust (WOT)	McAfee SiteAdvisor Plus	Được tải về hơn 33 triệu lần, trình bổ sung phổ biến này cho Firefox, Internet Explorer, Chrome, Safari hoặc Opera cho phép những người sử dụng biết khi nào họ bị lạc trong các website đáng ngờ hoặc không an ninh. Nó sử dụng việc xếp hạng người sử dụng để nhận diện các site luôn có những độc hại, thu thập thông tin cá nhân hoặc đưa vào các nội dung không phù hợp, và nó xếp hạng chúng với một hệ thống phân loại xanh-vàng-đỏ. Hệ điều hành: Windows, Linux, OS X.
	PasswordMaker	Kaspersky Password Manager, Roboform	Việc luôn luôn sử dụng cùng một mật khẩu sẽ đặt bạn vào rủi ro, nhưng nhiều người vẫn làm thế vì khó nhớ được nhiều mật khẩu khác nhau. Trình bổ sung cho trình duyệt này đưa ra một giải pháp tốt hơn cho vấn đề này bằng việc tạo những mật khẩu duy nhất cho từng site mà bạn viếng thăm và lưu trữ chúng trong một tệp được mã hóa mà bạn truy cập với một vấn đề mật khẩu duy nhất. Hệ điều hành: Windows, Linux, OS X.
Loại bỏ dữ liệu	BleachBit	Easy System Cleaner	Tiện ích hữu dụng này làm sạch máy chủ bạn để bảo vệ tính riêng tư và cải thiện hiệu năng. Nó giải phóng không gian đĩa bằng việc làm sách rác từ hơn 90 ứng dụng, xóa các tệp tạm thời, xóa bộ nhớ tạm và lịch sử duyệt, và "nghiền vụn" các tệp không mong muốn. Hệ điều hành: Windows, Linux.
	Eraser	BCWipe	Giống như BleachBit, Eraser "nghiền vụn" các tệp bị

Loại	Tên phần mềm	Thay thế cho	Mô tả
		Enterprise	xóa sao cho chúng không thể phục hồi lại được. Nó giúp bảo vệ những thông tin nhạy cảm bằng việc ghi đè các tệp bị xóa vài lần với các dữ liệu ngẫu nhiên. Hệ điều hành: Windows.
	Wipe	BCWipe Enterprise	Wipe đưa ra cùng chức năng như Eraser, nhưng nó là cho Linux thay vì cho Windows. Site này cũng đưa ra nhiều thông tin cho những ai quan tâm trong việc học nhiều hơn về cách mà tệp "nghiền vụn" làm việc. Hệ điều hành: Linux.
	Darik's Boot and Nuke	Kill Disk, BCWipe Total WipeOut	Trong khi Eraser và Wipe xóa các tệp duy nhát, thì DBAN xóa an toàn toàn bộ các đĩa. Nó rất hữu dụng khi tặng hoặc vứt bỏ một máy cũ. Hệ điều hành: Độc lập với hệ điều hành.
Chống mất dữ liệu	OpenDLP	RSA Data Loss Prevention Suite, CheckPoint DLP Software Blade, Symantec Data Loss Prevention Product Family	OpenLDAP là một "công cụ ngăn chặn mất dữ liệu phân tán mạnh, quản lý tập trung, dựa vào tác nhân hoặc không tác nhân". Nó cho phép những người quản lý an ninh hoặc tuân thủ quét hàng ngàn hệ thống cùng một lúc thông qua các tác nhân hoặc thực hiện sự phục hồi dữ liệu không tác nhân đối với máy chủ MySQL hoặc Microsoft SQL Server. Hệ điều hành: Windows.
	MyDLP	RSA Data Loss Prevention Suite, CheckPoint DLP Software Blade, Symantec Data Loss Prevention Product Family	MyDLP có thể khóa các số thẻ tín dụng, các số an ninh xã hội, hoặc các tệp nhạy cảm khỏi truyền được qua thư điện tử, các máy in, Web hoặc các thiết bị tháo lắp được. Bổ sung vào phiên bản cộng đồng tự do, nó cũng đi với một phiên bản doanh nghiệp phải trả tiền. Hệ điều hành: Windows, Linux, VMWare.
Mã hóa	AxCrypt	McAfee Anti-Theft, CryptoForge	Với gần 25 triệu người sử dụng đăng ký, AxCrypt được cho là "phần mềm mã hóa tệp hàng đầu của nguồn mở đối với Windows". Nó tích hợp với Windows Explorer - để sử dụng nó, bạn đơn giản hãy nháy chuột phải để mã hóa một tệp hoặc nháy đúp để giải mã. Hệ điều hành: Windows.
	Gnu Privacy Guard	PGP Universal Gateway Email Encryption	Dự án Gnu này là một triển khai dòng lệnh của tiêu chuẩn mã hóa phổ biến OpenPGP. Nó hỗ trợ các thuật toán mã hóa ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 và TIGER. Hệ điều hành: Linux.
	GPGTools	PGP Universal	Những người sử dụng Mác có thể tải về phiên bản GPG

Loại	Tên phần mềm	Thay thế cho	Mô tả
		Gateway Email Encryption	này cho một cách thức thân thiện hơn với người sử dụng để mã hóa thư điện tử và các tệp. Website này bao gồm một ít tài liệu trợ giúp cho những người sử dụng mới, làm cho nó thậm chí còn dễ hơn để làm quen sử dụng ứng dụng này. Hệ điều hành: OS X.
	gpg4win	Cypherus	Và phiên bản này đưa ra GPG cho những người sử dụng Windows, hoàn toàn với một giao diện người sử dụng đồ họa. Nó cài đặt nhanh và dễ dàng, và nó bảo vệ cả các tệp và để lại các thông điệp thư. Hệ điều hành: Windows.
	PeaZip	WinZip	Trong khi đây thực sự là một tiện ích nén chứ không phải là một công cụ mã hóa, thì PeaZip cũng đưa ra các khả năng mã hóa mạnh, mà giải thích vì sao chúng ta đã đưa nó vào phần này của danh sách. Nó cũng bao gồm các khả năng xác thực 2 yếu tố và xóa có an ninh. Hệ điều hành: Windows, Linux.
	Crypt	McAfee Anti-Theft, CryptoForge	Chỉ với 44KB, Crypt là một trong những tiện ích nhẹ cân nhất sẵn sàng. Và vì nó có thể mã hóa được 3MB giá trị dữ liệu chỉ trong vòng 0.7 giây, nó còn là một trong những tiện ích nhanh nhất. Tuy nhiên, nó không có một giao diện người sử dụng đồ họa, nên sẽ cần thuận tiện với dòng lệnh để sử dụng nó. Hệ điều hành: Windows.
	NeoCrypt	McAfee Anti-Theft, CryptoForge	NeoCrypt hỗ trợ nhiều thuật toán mã hóa, bao gồm AES, DES, Triple-DES, IDEA, RC4, RC5, CAST-128, BlowFish, SkipJack. Nó chạy từ một giao diện người sử dụng đồ họa dễ dàng sử dụng, và nó cũng tích hợp với Windows Shell sao cho bạn có thể mã hóa và giải mã các tệp ngày từ Windows Explorer. Hệ điều hành: Windows.
	LUKS/ cryptsetup	PGP Whole Disk Encryption	Ngắn gọn cho "Thiết lập Khóa Linux Thống nhất", LUKS tự gọi nó là "tiêu chuẩn cho mã hóa đĩa cứng trong Linux". Trong khi nhiều ứng dụng khác trong danh sách của chúng ta mã hóa từng tệp một, thì LUKS mã hóa toàn bộ đĩa của bạn. Hệ điều hành: Linux.
	FreeOTFE	PGP Whole Disk Encryption	Giống như LUKS, ứng dụng này mã hóa toàn bộ đĩa. Với nó bạn có thể tạo và mã hóa các đĩa ảo trong đĩa cứng của bạn. Nó cũng khả chuyển cao và có thể chạy từ một ổ USB. OS: Windows.

Loại	Tên phần mềm	Thay thế cho	Mô tả
	TrueCrypt	PGP Whole Disk Encryption	Một trong những lựa chọn mã hóa đĩa nguồn mở phổ biến, TrueCrypt có hơn 22 triệu bản tải về. Nhờ công nghệ song song hóa và đặt đường ống, nó đưa ra việc đọc và ghi thông tin mã hóa nhanh. Hệ điều hành: Windows.
Truyền tệp an ninh	WinSCP	CuteFTP, FTP Commander	Cực ký phổ biến, WinSCP được giải thưởng bao gồm máy trạm SFTP, máy trạm SCP, máy trạm FTPS và máy trạm FTP. Nó đưa ra 2 giao diện khác nhau và cũng bao gồm một trình soạn thảo văn bản tích hợp. Hệ điều hành: Windows.
	FileZilla	CuteFTP, FTP Commander	Trong khi WinSCP đưa ra chỉ một phiên bản máy trạm, thì FileZilla đưa ra cả phiên bản máy trạm và phiên bản cho phép bạn thiết lập máy chủ FTP của riêng bạn. Nó hỗ trợ các giao thức truyền FTP, FTPS và SSH. Hệ điều hành: Windows, Linux, OS X.
Điều tra pháp lý	ODESSA	EnCase Forensics, X-ways Forensics, AccessData Forensic Toolkit	Kiến trúc Chiếm đoạt và Tìm kiếm Bằng chứng Số Mở, còn gọi là "ODESSA", đưa ra vài công cụ khác nhau cho việc xem xét và báo cáo về bằng chứng số. Đây là một dự án cũ hơn, nhưng vẫn còn có giá trị. Hệ điều hành: Windows, Linux, OS X.
	The Sleuth Kit/ Autopsy Browser	EnCase Forensics, X-ways Forensics, AccessData Forensic Toolkit	Hai ứng dụng này làm việc cùng nhau: Sleuth Kit đưa ra các công cụ dòng lệnh cho việc tiến hành điều tra số, và Autospy Broser đưa ra một GUI dựa vào trình duyệt cho việc truy cập các công cụ đó. Dự án này bây giờ cũng một khung Hadoop cho phân tích dữ liệu phạm vi lớn. Hệ điều hành: Windows, Linux, OS X.
Cổng gateway / Thiết bị Quản lý Mối đe dọa Thống nhất	Endian Firewall Community	Check Point Security Gateways, SonicWall, Symantec Web Gateway	Cộng đồng Tường lửa Endian có thể biến bất kỳ PC nào (bao gồm cả những PC khá cũ) thành một thiết bị án ninh cổng gateway hoàn chỉnh với một tường lửa, các ủy quyền mức ứng dụng với hỗ trợ chống virus, lọc virus và spam cho thư điện tử, nội dung Web và một mạng riêng ảo VPN. Các phiên bản được hỗ trợ các thiết bị phần mềm và phần cứng cũng sẵn sàng trên site. Hệ điều hành: Linux.
	Untangle Lite	Check Point Security Gateways, SonicWall, Symantec Web	Tương tự như Endian, Untangle Lite cũng giúp những người sử dụng tạo các thiết bị an ninh cổng gateway của riêng họ. Bổ sung thêm, Untangle đưa ra các sản phẩm thương mại, và bạn có thể tải về mỗi trong số các ứng dụng riêng rẽ được đưa vào trong Untangle Lite (tường

Loại	Tên phần mềm	Thay thế cho	Mô tả
		Gateway	lửa, ngăn chặn thâm nhập trái phép, khóa các cuộc tấn công, ...) một cách tách biệt. Hệ điều hành: Linux.
	ClearOS	Check Point Security Gateways, SonicWall, Symantec Web Gateway	ClearOS kết hợp chức năng an ninh cổng gateway với các khả năng của một máy chủ doanh nghiệp nhỏ. Nó đưa ra việc kết nối mạng, phần mềm nhóm, một máy chủ thư, một máy chủ Web và hơn thế. Hỗ trợ có trả tiền và phần cứng cũng có sẵn. Hệ điều hành: Linux.
Dò tìm thâm nhập trái phép	Open Source Tripwire	Tripwire	Tripwire tiêu chuẩn bây giờ là một dự án nguồn đóng, nhưng cộng đồng đã tiếp tục phát triển phiên bản nguồn mở trong năm 2000. Nó giám sát nội dung và các tệp và cảnh báo cho những người quản lý mạng khi những tệp đó bị thay đổi, cảnh báo cho họ có những thâm nhập trái phép có khả năng. Hệ điều hành: Windows, Linux.
	OSSEC	Corero IPS, HP Tipping Point IPS, Sophos HIPS	Bổ sung thêm vào việc kiểm tra tính toàn vẹn của các tệp, OSSEC cũng thực hiện phân tích lưu ký, giám sát chính sách, dò tìm rootkit và cảnh báo thời gian thực để giúp ngăn ngừa và dò tìm thâm nhập trái phép trong mạng của bạn. Nó được tải về hơn 5.000 lần mỗi tháng và đã thắng nhiều giải thưởng. Hệ điều hành: Windows, Linux.
	AFICK	Tripwire	AFICK, ngắn gọn là "Trình Kiểm tra Tính toàn vẹn Tệp Khác", đưa ra chức năng tương tự như Tripwire. Nó khả chuyển, nhanh và chạy từ GUI hoặc dòng lệnh. Hệ điều hành: Windows, Linux.
	Snort	Corero IPS, HP Tipping Point IPS, Sophos HIPS	Với hàng triệu lượt tải về và hơn 400.000 người sử dụng đăng ký, Snort được cho là "Công nghệ IDS/IPS được triển khai rộng rãi nhất thế giới". Hệ điều hành: Windows, Linux, OS X.
Tường lửa mạng	IPCop	Barricuda NG Firewall, Check Point Appliances	Giống như hầu hết các ứng dụng khác trong danh sách các Tường lửa của chúng tôi, IPCop biến một PC thành một tường lửa dựa vào Linux để bảo vệ mạng của bạn. Nó được thiết kế cho những người sử dụng ở nhà hoặc SOHO, và nó có một giao diện Web dễ sử dụng. Hệ điều hành: Linux.
	Devil-Linux	Barricuda NG Firewall, Check Point Appliances	Dù nó ban đầu từng được thiết kế để đưa ra chức năng tường lửa và định tuyến router, thì Deviel - Linux cũng còn vận hành như một máy chủ cho nhiều ứng dụng, bao gồm cả đặt chỗ cho thư. Được các nhà quản trị CNTT

Loại	Tên phần mềm	Thay thế cho	Mô tả
			tạo ra cho các quản trị viên CNTT, nó có các khả năng tùy biến tuyệt vời và an ninh hàng đầu. Hệ điều hành: Linux.
	Turtle Firewall	Barricuda NG Firewall, Check Point Appliances	Được thiết kế để đơn giản và nhanh, Turtle cho phép các nhà quản lý mạng thiết lập cấu hình nó thông qua giao diện Web hoặc bằng việc sửa đổi các tệp XML. Website này cũng bao gồm một số thông tin giới thiệu tốt về bản chất tự nhiên của các tường lửa. Hệ điều hành: Linux.
	Shorewall	Barricuda NG Firewall, Check Point Appliances	Shorewall không được cho là tường lửa Linux dễ sử dụng nhất, nhưng nó được cho là "tường lửa mềm dẻo và mạnh nhất". Bạn có thể sử dụng nó trong một hệ thống vận hành như một tường lửa chuyên dụng, như một cổng gateway/bộ định tuyến router/máy chủ đa chức năng hoặc như một chiếc PC GNU/Linux đứng riêng rẽ. Hệ điều hành: Linux.
	Vuurmuur	Barricuda NG Firewall, Check Point Appliances	Vuurmuur được thiết kế để trở nên đơn giản và mạnh. Bổ sung thêm vào các khả năng tường lửa tiêu chuẩn, nó cũng hỗ trợ việc làm sắc sảo giao thông và đưa ra những khả năng giám sát tiên tiến. Hệ điều hành: Linux.
	m0n0wall	Barricuda NG Firewall	Mặc dù nó đã được thiết kế cho các thiết bị và máy tính cá nhân PC nhúng, thì m0n0wall cũng có thể chạy được trên một PC đứng riêng rẽ chạy FreeBSD. Nó đòi hỏi ít hơn 12MB không gian đĩa và khởi động ít hơn 25 giây. Hệ điều hành: FreeBSD.
	pfSense	Barricuda NG Firewall, Check Point Appliances	Rẽ nhánh này của m0n0wall cũng dựa vào BSD, nhưng được thiết kế cho các máy tính thông thường, không phải phần cứng nhúng. Nó được tải về hơn 1 triệu lần và hiện chạy trên hơn 100.000 mạng, bao gồm cả các tập đoàn và các trường đại học lớn cũng như các mạng nhỏ ở nhà. Hệ điều hành: FreeBSD.
	Vyatta	Cisco products	Phần mềm Vyatta "lõi" cho phép những người sử dụng tạo ra những thiết bị và các bộ định tuyến router mạng/tường lửa của riêng họ. Công ty này cũng đưa ra các phần cứng và mềm phải trả tiền. Hệ điều hành: Linux.
Giám sát mạng	Wireshark	OmniPeek, CommView	Tự gọi mình là "Trình phân tích giao thức mạng đầu tiên trên thế giới", Wireshark làm cho dễ dàng để nắm bắt và phân tích giao thông mạng. Các sản phẩm và dịch vụ thương mại có liên quan tới phần mềm đó là sẵn sàng

Loại	Tên phần mềm	Thay thế cho	Mô tả
			thông qua Riverbed Technology. Hệ điều hành: Windows, Linux, OS X.
	Tcpdump/ libpcap	OmniPeek, CommView,	Tcpdump là một trình phân tích gói dùng dòng lệnh, và libpcap là một thư viện C/C++ cho nắm bắt giao thông mạng. Làm việc cùng nhau, 2 thứ này cung cấp một giải pháp giám sát mạng tốt, nhưng, thiếu một GUI, chúng không thực sự thân thiện với người sử dụng. Hệ điều hành: Linux.
	WinDump	OmniPeek, CommView	Được Riverbed Technology quản lý (còn được gọi là Wireshark), WinDump chuyển tcpdump tới nền tảng Windows. Site này cũng bao gồm thư viện và các trình điều khiển WinPcap cho nắm bắt giao thông. Hệ điều hành: Windows.
Phá mật khẩu	Ophcrack	Access Data Password Recovery Toolkit, Passware	Cùng với thời gian, mỗi người cần phục hồi lại một mật khẩu bị mất hoặc không biết. Trình phá mật khẩu này sử dụng phương pháp các bảng cầu vồng để phục hồi các mật khẩu không biets, và nó cũng bao gồm module ép mạnh thô bạo cho các mật khẩu đơn giản. Hệ điều hành: Windows.
	John the Ripper	Access Data Password Recovery Toolkit, Passware	John the Ripper là đặc biệt tốt để phá các mật khẩu yếu, nhưng để sử dụng nó, bạn sẽ cần một danh sách các mật khẩu thường được sử dụng. Bạn có thể mua các danh sách mật khẩu hoặc một phiên bản chuyên nghiệp các phần mềm từ cùng site này. Hệ điều hành: Windows, Linux, OS X.
Quản lý mật khẩu	KeePass Password Safe	Kaspersky Password Manager	Trình quản lý mật khẩu phổ biến này lưu trữ tất cả các mật khẩu của bạn trong một cơ sở dữ liệu được mã hóa. Bạn sẽ chỉ cần nhớ một mật khẩu chủ, trong khi ứng dụng dễ sử dụng, nhẹ này sẽ giúp bạn bảo vệ bạn khỏi bọn ăn cắp nhận diện. Hệ điều hành: Windows.
	KeePassX	Kaspersky Password Manager	Nếu bạn sử dụng OS X hoặc Linux, hãy thử rẽ nhánh này của KeePass. Cộng với, nó bổ sung một ít tính năng không có ban đầu và chạy được cả trong Windows. Hệ điều hành: Windows, Linux, OS X
	Password Safe	Kaspersky Password Manager	Được tải về hơn 1 triệu lần, Password Safe là một lựa chọn nguồn mở phổ biến khác cho việc bảo vệ các mật khẩu của bạn. Giống như KeePass, nó là nhẹ và lưu trữ các mật khẩu được mã hóa của bạn trong một cơ sở dữ liệu sao cho bạn chỉ cần nhớ một mật khẩu chủ. Hệ điều

Loại	Tên phần mềm	Thay thế cho	Mô tả
			hành: Windows.
Xác thực người sử dụng	WiKID	Entrust IdentityGuard, Vasco Digipass, RSA's SecurID	WiKID khoe về "xác thực 2 yếu tố mà không cần yếu tố nhiễu". Bổ sung vào phiên bản cộng đồng tự do, nó cũng có một phiên bản doanh nghiệp được hỗ trợ mà cũng bổ sung thêm chức năng. Hệ điều hành: Độc lập với hệ điều hành.
Lọc Web	DansGuardian	McAfee Family Protection, NetNanny, CyberPatrol	Bộ lọc nội dung có giải thưởng này sử dụng việc khớp các mệnh đề, lọc PICS, lọc URL và các phương pháp khác để khóa nội dung bị phản đối. Lưu ý là phần mềm này không chạy trên các máy tính cá nhân riêng rẽ. Nó chạy trên một máy chủ OS X hoặc Linux để bảo vệ phần còn lại của mạng. Hệ điều hành: Linux, OS X.

10.2. Danh sách 12 phần mềm tự do nguồn mở sử dụng trong an ninh

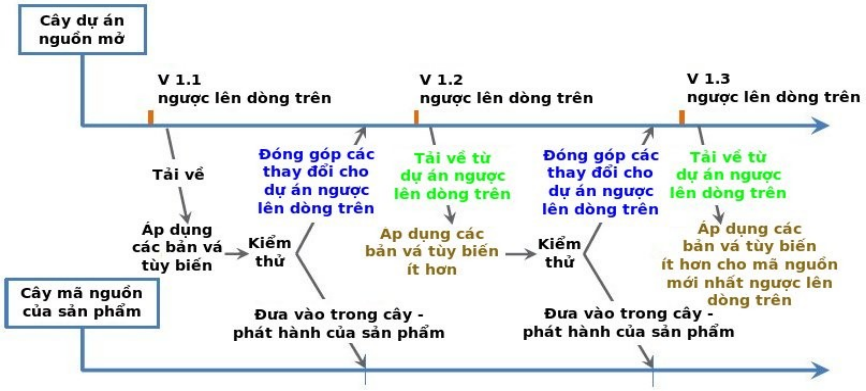
Loạt bài của Carla Schroder về 12 phần mềm tự do nguồn mở tuyệt vời trong lĩnh vực an ninh mà bạn có thể sử dụng để thay thế các ứng dụng sở hữu độc quyền. Xem các phần [01], [02], [03], [04], [05].

Loại	Tên phần mềm	Thay thế cho	Mô tả
Xóa có an ninh, khôi phục dữ liệu, nhái lại, mã hóa	Darik's Boot and Nuke (DBAN)	BCWipe Total WipeOut, Secure Erase, HDShredder	DBAN là hệ điều hành độc lập và làm việc trong các ổ cứng IDE, SCSI và SATA trên các hệ thống x86 và PowerPC. DBAN dễ sử dụng: tải về và sao chép vào vật trung gian khởi động được như đĩa mềm 3.5", CD/DVD, đầu USB hoặc PXE khởi động qua một mạng - chạy nó và để nó làm. Bạn có thể quét sạch tất cả các đĩa cứng trong một hệ thống, hoặc chỉ những thứ được chọn.
Sửa và phục hồi tệp	TestDisk and PhotoRec	Recover Lost Partition, Active@ Partition Recovery, Disk Doctors	Bạn có thể cài đặt chúng lên hầu như bất kỳ hệ điều hành nào (Mac, Linux, Windows, BSD và các Unix khác), nhưng cách tốt nhất để chạy chúng là từ vật trung gian khởi động được. TestDisk và PhotoRec được đưa vào trong một số lượng lớn các phát tán cứu hệ thống dựa vào Linux như GParted LiveCD và Knoppix.
Cứu các ổ đĩa hỏng	GNU ddrescue	Norton Ghost, Acronis True Image, Paragon Backup & Recovery	ddrescue thực hiện các bảo sao ở mức khối bloc, nên không là vấn đề gì đối với hệ thống tệp hoặc hệ điều hành đang trong vật trung gian. Nó nhanh vì nó sao chép chỉ các khối còn tốt và bỏ qua các khối hỏng, và nó là tự động nên bạn không phải chăm sóc gì. Thiết bị bạn đang sao chép tới, như một đĩa USB hoặc đĩa cứng nội bộ thứ 2, nên rộng lớn hơn 50% so với đĩa gốc.
Nhái	Clonezilla	Norton Ghost và	Có 2 phiên bản: Clonezilla Live và Clonezilla SE.

Loại	Tên phần mềm	Thay thế cho	Mô tả
đĩa		Symantec Ghost Corporate Edition	Clonezilla Live là cho sao lưu và phục hồi các máy tính riêng rẽ, và nó chạy từ một đầu USB khởi động được hoặc CD/DVD. Clonezilla SE nhái nhiều máy tính cá nhân cùng một lúc, và rất nhanh qua mạng của bạn. Clonezilla vận hành ở mức khối trên các nền tảng x86 và x86-64, nên nó sao chép bất kỳ hệ thống tập và hệ điều hành nào.
Mã hóa	TrueCrypt	PGP Whole Disk Encryption	Là một trong những ứng dụng mã hóa liên nền tảng phổ biến nhất, và vì lý do tốt lành - nó dễ dàng sử dụng và rất mạnh. TrueCrypt chạy trong Mac, Linux và Windows.
An ninh di động	Master Password (iOS)	Password Safe	Master Password cho iOS là một trình quản lý mật khẩu không tình trạng. Nó không lưu các mật khẩu vào iPhone/Pad/Pod, cũng không lưu chúng trong một vài chỗ đâu đó trong đám mây mờ đục. Nó triển khai một chiến lược khác: nó tạo ra một mật khẩu mới, mạnh mỗi lần bạn cần đăng nhập vào một site. Bạn chỉ cần nhớ một mật khẩu duy nhất. (Giá 5.99 USD)
	Secure Chat		ChatSecure mã hóa AIM, Jabber, Google Talk, và tất cả các ứng dụng chat/IM apps mà sử dụng giao thức chat XMPP.
	Rights Alert		Rights Alert chỉ cho bạn một danh sách các ứng dụng được cài đặt mà đang yêu cầu các quyền thừa quá mức, có thể là một dấu hiệu rằng chúng có thể sẽ không tốt, mò mẫm và tọc mạch vào trong các phần hệ thống của bạn nơi mà chúng không thuộc về.
	Dự án Guardian		Dự án Guardian là một bộ các ứng dụng nguồn mở bảo vệ tính riêng tư đã được tạo ra với ý tưởng bảo vệ các nhà hoạt động chính trị xã hội mà đang gặp nguy hiểm đơn giản báo các sự kiện và chia sẻ các ảnh, và tất nhiên các ứng dụng đó làm việc cho bất kỳ ai mà có quan tâm về tính riêng tư của họ trên trực tuyến.
	Orbot		Orbot mang Tor vào Android. Tor là mạng các máy chủ ủy quyền nặc danh hóa các cuộc du lịch của bạn trên Internet
	Gibberbot		Gibberbot đưa ra thông điệp tức thì và chat an ninh, với phần thưởng của sự hỗ trợ của Tor.
	Droidwall		Droidwall là một giao diện mặt tiền đồ họa đẹp cho tường lửa mạnh và được chứng minh Iptables từng là

Loại	Tên phần mềm	Thay thế cho	Mô tả
			một phần không thể thiếu của nhân Linux trong nhiều năm. Nó trao sự kiểm soát tốt đối với các ứng dụng và dịch vụ có thể có sự truy cập tới các mạng của bạn, và kiểm soát những gì tới Droid của bạn qua mạng.

10.3. Tuân thủ mô hình phát triển cộng đồng cho phần mềm nguồn mở

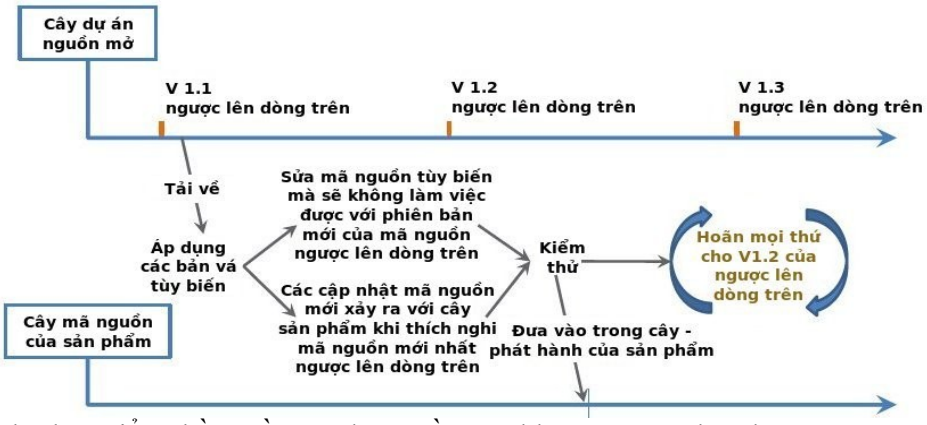


Mô hình phát triển phần mềm tự do nguồn mở có ngược lên dòng trên.

Khi sử dụng các phần mềm an ninh là phần mềm tự do nguồn mở, việc tùy biến các phần mềm đó nên được thực hiện theo đúng mô hình phát triển của phần mềm tự do nguồn mở để đảm bảo các phần mềm đó luôn được cập nhật nhanh chóng, đúng thời hạn, qua đó đảm bảo được an ninh cho hệ thống. Tránh việc tùy biến mã nguồn của phần mềm rồi đem đóng lại, không chuyển mã nguồn tùy biến ngược lên dòng trên về với dự án gốc của phần mềm.

Thường thì khi không ngược lên dòng trên để đóng góp mã nguồn được tùy biến trở về với dự án dòng chính thống, thì ta sẽ có các phiên bản rẽ nhánh của phần mềm đó và khó hoặc không thể nhận được những đóng góp của cả cộng đồng dự án cho bản rẽ nhánh đó. Kết quả là sau một thời gian, phần mềm rẽ nhánh có khả năng bị lạc hậu, gây mất an ninh cho hệ thống.

Nói như vậy không có nghĩa là không bao giờ được rẽ nhánh, mà chỉ rẽ nhánh khi thực sự cần thiết và chuẩn bị đầy đủ về cả nhân lực và vật lực để có thể duy trì kho mã nguồn của phần mềm rẽ nhánh đó.



Mô hình phát triển phần mềm tự do nguồn mở không ngược lên dòng trên - rẽ nhánh.

Các tài liệu tham khảo:

1. An ninh không gian mạng - Câu hỏi gây tranh cãi đối với các quan hệ toàn cầu. Một báo cáo độc lập về sự chuẩn bị sẵn sàng về không gian mạng trên thế giới. Chương trình nghị sự về An ninh & Phòng thử (SDA) xuất bản tháng 02/1012, 94 trang. Tải về.
2. Phát triển công nghệ mở. Những bài học học được và những thực tiễn tốt nhất cho các phần mềm quân sự, phiên bản 1.0. Bộ Quốc phòng Mỹ. Xuất bản 16/05/2011. 73 trang. Tải về.
3. Kế hoạch lộ trình phát triển công nghệ mở, phiên bản 3.1. Bộ Quốc phòng Mỹ. Tháng 07/2006. 59 trang. Tải về.
4. Các tác chiến thông tin. Học thuyết về tác chiến thông tin của Mỹ và Liên quân. Bộ Quốc phòng Mỹ. Xuất bản 13/02/2006. 119 trang.Tải về.
5. Khả năng của Cộng hòa Nhân dân Trung hoa tiến hành chiến tranh không gian mạng và khai thác mạng máy tính. Tập đoàn Northrop Grumman xuất bản ngày 09/10/2009. 75 trang.Tải về.
6. Nga, Mỹ và ngoại giao không gian mạng - Các cánh cửa còn để ngỏ. Viện Đông - Tây xuất bản năm 2010. 32 trang.Tải về.
7. Báo cáo thường niên cho Quốc hội - Diễn biến về quân sự và an ninh liên quan tới Cộng hòa Nhân dân Trung Hoa 2011, Văn phòng Bộ trưởng Quốc phòng Mỹ, Bộ Quốc phòng Mỹ. Xuất bản 06/05/2011. 94 trang.Tải về.
8. Những thách thức trong không gian mạng, Viện về Phân tích Quốc phòng (IDA), Bộ Quốc phòng Mỹ, xuất bản mùa hè năm 2011. 24 trang.Tải về.
9. Chiến lược về tác chiến trong không gian mạng, Bộ Quốc phòng Mỹ xuất bản tháng 07/2011. 19 trang.Tải về.
10. Chiến lược An ninh Không gian mạng của nước Anh, Bảo vệ và thúc đẩy nước Anh trong thế giới số, tháng 11/2011, Văn phòng Nội các Chính phủ Anh, 43 trang.Tải về.
11. Những mối đe dọa không gian mạng đang nổi lên và quan điểm của Nga về chiến tranh thông tin và tác chiến thông tin. Cơ quan Nghiên cứu Quốc phòng FOI, Thụy Điển, 2010. 70 trang. Tải về.
12. Chỉ dẫn về an ninh cho các lĩnh vực trọng tâm sống còn trong ĐTĐM v2.1 của Liên minh An ninh Đám mây CSA, xuất bản tháng 12/2009, 72 trang. Tải về.
13. Lộ trình Công nghệ Điện toán Đám mây của Chính phủ Mỹ, Tập 1, phiên bản 1.0 (Dự thảo). Các yêu cầu ưu tiên cao để áp dụng hơn nữa Điện toán Đám mây của các cơ quan Chính phủ Mỹ. Chương trình Điện toán Đám mây, Phòng Thí nghiệm Công nghệ Thông tin, Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ - NIST. Tháng 11/2011. 32 trang.Tải về.
14. Kiến trúc tham chiếu Điện toán Đám mây của NIST. Những khuyến cáo của Viện Tiêu chuẩn và Công nghệ Quốc gia. Viện Tiêu chuẩn và Công nghệ Quốc gia, Mỹ - NIST. Tháng 09/2011. 35 trang. Tải về.
15. Lộ trình tiêu chuẩn Điện toán Đám mây của NIST v1.0. Viện Tiêu chuẩn và Công nghệ Quốc gia, Mỹ - NIST. Tháng 07/2011. 76 trang. Tải về.
16. Bản ghi nhớ cho các giám đốc thông tin - Ủy quyền an ninh của các hệ thống thông tin trong các môi trường điện toán đám mây. Steven VanRoekel, Giám đốc Thông tin Liên bang Mỹ, Văn phòng Điều hành của Tổng thống Mỹ, xuất bản ngày 08/12/2011. 7 trang. Tải về.
17. Chuẩn và Kiến trúc cho các ứng dụng chính phủ điện tử, phiên bản v2.0. Bộ Nội vụ Cộng hòa Liên bang Đức xuất bản. Tháng 12/2003. 179 trang. Tải về.
18. Chuẩn và Kiến trúc cho các ứng dụng chính phủ điện tử, phiên bản v3.0. Bộ Nội vụ Cộng hòa

Liên bang Đức xuất bản. Tháng 10/2006. 185 trang. Tải về.
19. Ngược lên dòng trên: Tăng cường cho sự phát triển nguồn mở. Quỹ Linux. Tháng 01/2012. 10 trang. Tải về.
20. Mua sắm phần mềm máy tính của Chính phủ và Giấy phép Công cộng Chung GNU, B. Scott Michel, Lt. Cmdr., PhD, USN(RC), Eben Moglen, Trung tâm Luật Tự do cho Phần mềm, Mishi Choudhary, Trung tâm Luật Tự do cho Phần mềm, Dorothy Becker, Luật sư về Bằng sáng chế, SPD của Navy OGC. Xuất bản ngày 01/10/2011, 15 trang. Tải về.

Ghi chú: Một số thông tin tham khảo khác về an ninh được cập nhật hàng ngày có thể xem ở đây, ở đây hoặc ở đây.