BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC, KỸ NĂNG BẢO ĐẢM AN TOÀN THÔNG TIN CHO THIẾT BỊ DI ĐỘNG, THIẾT BỊ THÔNG MINH"

Hà Nội, năm 2023

CHƯƠNG 1. CÁC LOẠI THIẾT BỊ DI ĐỘNG, THIẾT BỊ THÔNG MINH

1.1. Các loại thiết bị di động

1.1.1. Định nghĩa Thiết bị di động

Thiết bị di động là một loại thiết bị điện tử di động có khả năng di chuyển và thực hiện các chức năng có thể tương đương với các máy tính và thiết bị điện tử khác, thường được sử dụng trong cuộc sống hàng ngày. Thiết bị di động bao gồm một loạt các sản phẩm, chủ yếu là điện thoại di động (smartphones) và máy tính bảng, nhưng cũng có thể bao gồm các thiết bị khác như đồng hồ thông minh, tai nghe thông minh, và các thiết bị đeo sức khỏe.

Đặc điểm chung của thiết bị di động là khả năng di động, tích hợp nhiều chức năng trong một thiết bị, và khả năng kết nối với Internet. Thiết bị di động thường sử dụng hệ điều hành di động để thực hiện các nhiệm vụ và chạy ứng dụng, và chúng thường có màn hình cảm ứng để tương tác người dùng.

Các tính năng chính của thiết bị di động mang lại điển hình như: giao tiếp, truy cập Internet, giải trí, chụp ảnh và quay video, quản lý lịch trình và ghi chú, định vị và bản đồ, ứng dụng công việc và giáo dục, chăm sóc sức khỏe, sử dụng ứng dụng thanh toán để thực hiện các giao dịch tài chính, cung cấp xác thực sinh trắc học như nhận dạng khuôn mặt hoặc nhận dạng vân tay… Thiết bị di động đã trở thành một phần quan trọng và không thể thiếu trong cuộc sống hiện đại, mang lại sự thuận tiện và kết nối liên tục cho người sử dụng.

Liệt kê các nhà sản xuất thiết bị di động lớn trên toàn cầu, chúng ta thường nhắc đến những cái tên như: Apple, Samsung, Sony, Google, HTC, LG, Motorola Mobility và Nokia.

1.1.2. Sự phát triển và công dụng

Sự phát triển của thiết bị di động đã là một trong những diễn biến đáng kể nhất trong lĩnh vực công nghệ trong suốt nhiều năm qua.

Vào thập kỷ 1970 - 1980, xuất hiện các mô hình đầu tiên của điện thoại di động, như Motorola DynaTAC 8000X (1973) và Nokia Mobira Talkman (1984), kích thước lớn, trọng lượng nặng và chức năng giới hạn.

Thập kỷ 1990 - 2000, sự xuất hiện của điện thoại thông minh như IBM Simon (1992) và Nokia 9000 Communicator (1996), có những chức năng mở rộng với khả năng kết nối Internet và gửi email.

Sự ra đời của hệ điều hành di động bắt đầu từ những năm 2000 - 2010, như Symbian, BlackBerry OS, iOS (2007), và Android (2008), điện thoại thông minh trở thành một trung tâm giải trí di động với cộng đồng ứng dụng ngày càng phát triển.

Thập kỷ 2010-2020 là giai đoạn bùng nổ công nghệ cảm ứng, công nghệ cảm ứng trở nên phổ biến, cung cấp trải nghiệm người dùng tốt hơn, với màn hình lớn, độ phân giải cao, và camera chất lượng cao trở thành xu hướng chính.

Giai đoạn cuối thập kỷ 2000-2020, sự phổ cập Internet di động và công nghệ mạng 4G giúp tăng tốc độ kết nối và trải nghiệm người dùng, ứng dụng trực tuyến và dịch vụ đám mây trở nên phổ biến.

Cho đến nay, là sự phát triển mạnh mẽ của thiết bị thông minh khác nhau ngoài điện thoại, như đồng hồ thông minh, tai nghe thông minh, và thiết bị đeo sức khỏe, trí tuệ nhân tạo, thực tế ảo, và thực tế ảo trở nên ngày càng tích hợp. Công nghệ 5G cung cấp tốc độ Internet siêu nhanh, tăng khả năng kết nối và trải nghiệm người dùng. Thiết bị di động ngày càng trở thành trung tâm quản lý cho các thiết bị IoT trong cuộc sống hàng ngày.

Có thể thấy rằng, sự phát triển của thiết bị di động đã đưa đến những thay đổi đáng kể trong cách chúng ta giao tiếp, làm việc, giải trí, và quản lý cuộc sống hàng ngày. Các xu hướng công nghệ tiếp theo có thể sẽ tiếp tục mở ra những cơ hội mới và làm thay đổi cách chúng ta tương tác với thế giới xung quanh.

Dưới đây là một số công dụng quan trọng mà thiết bị di động mang lại:

1. Giao tiếp: thiết bị di động cho phép người dùng thực hiện cuộc gọi điện thoại và gửi tin nhắn một cách thuận tiện.

2. Truy cập Internet: thiết bị di động giúp người dùng truy cập Internet, duyệt web, và sử dụng email mọi lúc, mọi nơi.

3. Mạng xã hội: người dùng có thể kết nối với bạn bè và gia đình, chia sẻ thông tin qua các ứng dụng mạng xã hội như Facebook, Instagram, Twitter.

4. Giải trí di động: thiết bị di động cho phép người dùng nghe nhạc, xem video, và thậm chí là stream nội dung trực tuyến từ các dịch vụ như Youtube, các ứng dụng xem phim trực tuyến.

5. Chụp ảnh và quay video: thiết bị di động thường được trang bị camera, giúp người dùng chụp ảnh và quay video mọi lúc.

6. Quản lý lịch trình và ghi chú: thiết bị di động có thể giúp người dùng quản lý lịch trình, tạo ghi chú, và thiết lập bộ nhắc.

7. Định vị và bản đồ: thiết bị di động có thể sử dụng GPS để định vị vị trí và cung cấp bản đồ, hướng dẫn điều hướng.

8. Mua sắm trực tuyến: người dùng có thể mua sắm trực tuyến, so sánh giá, và đặt hàng từ các ứng dụng mua sắm.

9. Ngân hàng di động: cho phép người dùng kiểm tra số dư, chuyển khoản và thực hiện các giao dịch ngân hàng trực tuyến.

10. Giáo dục và học tập: cung cấp truy cập vào tài liệu giáo dục, ứng dụng học ngoại ngữ, và các tài nguyên giáo dục trực tuyến.

11. Sức khỏe và thể dục: cung cấp các ứng dụng theo dõi sức khỏe, bước chân, và giúp người dùng duy trì lối sống lành mạnh.

12. Ứng dụng công việc: cho phép người dùng quản lý công việc, lịch trình làm việc, và tương tác với đồng nghiệp.

13. Quảng cáo và marketing: đưa doanh nghiệp và người tiêu dùng tiếp cận thông tin quảng cáo và chiến lược tiếp thị.

14. Chơi game di động: thiết bị di động là nền tảng chơi game phổ biến với nhiều thể loại và chất lượng đa dạng.

15. Thực hiện các giao dịch tài chính: cho phép thanh toán hóa đơn, chuyển tiền, và thực hiện các giao dịch tài chính.

Thiết bị di động đã trở thành một phần không thể thiếu của cuộc sống hiện đại, mang lại nhiều tiện ích và cơ hội tiếp cận thông tin một cách nhanh chóng và thuận tiện.

1.1.3. Các loại thiết bị di động

Có nhiều loại thiết bị di động khác nhau, với mỗi loại đều có những chức năng và ứng dụng riêng biệt. Dưới đây là một danh sách các loại thiết bị di động phổ biến:

- Điện thoại di động (Smartphones):

Bao gồm các mô hình từ nhiều nhà sản xuất như Apple, Samsung, Huawei, Xiaomi. Bao gồm các chức năng cuộc gọi, tin nhắn, truy cập Internet, chụp ảnh, quay video, cài đặt ứng dụng…

- Máy tính bảng (Tablets):

iPad của Apple, Samsung Galaxy Tab, Microsoft Surface, cho phép truy cập Internet, xem video, đọc sách điện tử, chơi game, công việc văn phòng.

- Đồng hồ thông minh (Smartwatches):

Apple Watch, Samsung Galaxy Watch, Fitbit. Hỗ trợ theo dõi sức khỏe, đo nhịp tim, thông báo từ điện thoại, xem thông tin thời tiết.

- Tai nghe thông minh (Smart Headphones):

AirPods của Apple, Samsung Galaxy Buds, Sony WH-1000XM4 cung cấp tính năng như nghe nhạc, cuộc gọi, điều khiển bằng cử chỉ, hủy tiếng ồn.

- Máy nghe nhạc di động (Portable Media Players):

iPod của Apple, Sony Walkman, SanDisk Clip Jam giúp chúng ta trải nghiệm tốt hơn với các chức năng nghe nhạc, xem video, lưu trữ và phát các tệp đa phương tiện.

- Máy đọc sách điện tử (E-readers):

Kindle của Amazon, Kobo, Nook của Barnes & Noble, phục vụ việc đọc sách điện tử, tải và lưu trữ nhiều sách.

- Máy chơi trò chơi di động (Gaming Devices):

Nintendo Switch, PlayStation Portable (PSP), các điện thoại chơi game.

- Thiết bị đeo sức khỏe (Wearable Health Devices):

Fitbit, Xiaomi Mi Band, Garmin công dụng theo dõi hoạt động, đo nhịp tim, đo chất lượng giấc ngủ.

- Máy ảnh và máy quay di động (Mobile Cameras):
- Máy tính xách tay (Laptops) và Máy tính bảng hai trong một (2-in-1 Tablets):

1.2. Các loại thiết bị thông minh

Thiết bị thông minh là một thiết bị điện tử, nói chung kết nối với các thiết bị khác hoặc thông qua mạng không dây khác nhau về giao thức như Bluetooth, NFC, Wi-Fi, 4G.., có thể hoạt động một số phạm vi tương tác và tự chủ. Một số loại thiết bị đáng chú ý bao gồm điện thoại thông minh, điện thoại lai và máy tính bảng, đồng hồ thông minh, vòng đeo thông minh và chuỗi khóa thông minh...

Thiết bị thông minh là bước tiến vượt bậc giúp cuộc sống của mỗi người chúng ta ngày càng hiện đại. Các thiết bị không những có thể điều khiển qua công tắc mà còn qua giọng nói, iPad,...

Một số ví dụ về các loại thiết bị thông minh:

1. Điện thoại thông minh (Smartphone): Điện thoại thông minh đã trở thành một công cụ không thể thiếu trong cuộc sống hiện đại. Nó không chỉ là một phương tiện liên lạc, mà còn là một thiết bị đa chức năng cho phép người dùng truy cập Internet, gửi nhận email, chơi game, xem phim, nghe nhạc và thực hiện nhiều nhiệm vụ khác.

2. Máy tính bảng (Tablet): Máy tính bảng là một thiết bị di động có kích thước lớn hơn điện thoại thông minh và được sử dụng chủ yếu để đọc sách, xem

phim, duyệt web và chơi game. Với màn hình cảm ứng và khả năng kết nối Internet, máy tính bảng trở thành công cụ hữu ích cho việc làm việc và giải trí.

3. Đồng hồ thông minh (Smartwatch): Đồng hồ thông minh là một thiết bị đeo tay kết hợp tính năng của một đồng hồ và một điện thoại thông minh. Nó cho phép người dùng đọc tin nhắn, cuộc gọi, kiểm tra email, theo dõi hoạt động thể dục và nhiều tính năng khác mà không cần lấy điện thoại ra khỏi túi.

4. Loa thông minh (Smart Speaker): Loa thông minh là thiết bị kết hợp với trí tuệ nhân tạo (AI) và các trợ lý ảo như Google Assistant, Amazon Alexa hoặc Apple Siri. Chúng cho phép người dùng tương tác giọng nói và điều khiển các thiết bị thông minh khác trong nhà, nghe nhạc, tra cứu thông tin và thực hiện các tác vụ thông qua lệnh giọng.

5. TV thông minh (Smart TV): TV thông minh là một phiên bản nâng cấp của TV truyền thống, có khả năng kết nối Internet và truy cập vào các ứng dụng và dịch vụ trực tuyến như Netflix, YouTube, Spotify và nhiều nội dung giải trí khác. Chúng cũng có thể được điều khiển bằng giọng nói hoặc điều khiển từ xa thông qua ứng dụng di động.

6. Thiết bị định vị thông minh (Smart GPS): Thiết bị định vị thông minh được sử dụng để xác định vị trí và định tuyến. Nó có thể cung cấp hướng dẫn chi tiết cho người dùng khi đi đến một địa điểm cụ thể và cung cấp thông tin về lưu lượng giao thông và các điểm quan trọng trên đường đi.

7. Thiết bị điều khiển thông minh (Smart Home Hub): Thiết bị điều khiển thông minh được sử dụng để kiểm soát các thiết bị thông minh khác trong nhà, như đèn, máy lạnh, hệ thống an ninh và các thiết bị gia đình khác. Chúng cho phép người dùng điều khiển và tự động hóa các

Nói cách khác, các thiết bị thông minh thuộc mạng lưới Internet of Things (IoT) là tập hợp các thiết bị có khả năng kết nối với nhau và kết nối với Internet.

CHƯƠNG 2. CÁC NGUY CƠ MẤT AN TOÀN ĐỐI VỚI THIẾT BỊ DI ĐỘNG, THIẾT BỊ THÔNG MINH

Sự gia tăng của thiết bị di động và thiết bị thông minh đã mang lại nhiều tiện ích và thuận lợi cho cuộc sống hàng ngày, nhưng cũng đồng thời đặt ra những thách thức lớn trong lĩnh vực bảo mật.

Số lượng thiết bị di động và thiết bị thông minh đã tăng vọt, không chỉ trong số lượng mà còn trong sự đa dạng về loại hình và chức năng. Thiết bị liên tục kết nối với Internet và với nhau, tạo ra môi trường kết nối liên tục và tương tác. Sự phát triển của ứng dụng và dịch vụ thông minh mở rộng khả năng sử dụng và tích hợp các thiết bị vào cuộc sống hàng ngày. Các hệ thống Internet of Things (IoT) và nhà thông minh tích hợp nhiều thiết bị khác nhau để tạo ra môi trường số thông minh. Sự gia tăng của phong cách sống kỹ thuật số đã làm tăng cường sự phụ thuộc và sử dụng các thiết bị di động và thông minh trong mọi lĩnh vực của cuộc sống…

Tất cả các yếu tố trên cho thấy, sự gia tăng về số lượng và tính phức tạp của các thiết bị tăng cường rủi ro an ninh, từ việc tấn công mạng đến việc xâm phạm quyền riêng tư cá nhân. Tấn công có thể diễn ra từ nhiều nguồn, từ malware truyền thống đến tấn công mục tiêu chuyên sâu và tấn công mạng lưới IoT. Dữ liệu cá nhân được thu thập từ các thiết bị thông minh có thể trở thành mục tiêu của tấn công, đặt ra lo ngại về quản lý và bảo vệ dữ liệu. Ứng dụng di động và các ứng dụng của thiết bị thông minh có thể chứa lỗ hổng bảo mật, tạo điểm vào hệ thống cho hacker. Người dùng và những người quản lý thường chưa đủ nhận thức về các rủi ro an ninh và cách bảo vệ chúng. Quản lý thông tin từ nhiều nguồn và tích hợp chúng đòi hỏi các biện pháp an ninh mạnh mẽ để ngăn chặn sự xâm phạm và lưu trữ an toàn. Việc quản lý chấp thuận từ phía người dùng và giữ cho họ được thông tin về việc sử dụng dữ liệu của họ là một thách thức.

Để hiểu rõ hơn về những nguy cơ và thách thức trong việc bảo đảm an toàn cho thiết bị di động và thiết bị thông minh. Chương này sẽ chia thành 2 phần: Nguy cơ mất an toàn đối với thiết bị di động và Nguy cơ mất an toàn đối với thiết bị thông minh.

2.1. Nguy cơ mất an toàn đối với thiết bị di động

Trong những năm gần đây, sự phổ biến của các thiết bị di động như điện thoại thông minh và máy tính bảng đã mang lại cho người dùng nhiều tiện lợi và khả năng dễ dàng sử dụng kết nối Internet mọi lúc, mọi nơi. Theo báo cáo của Hiệp hội Di động Toàn cầu (GSMA), cuối năm 2017, thế giới đã vượt qua mốc hơn 5 tỷ người sử dụng thiết bị di động. Tuy nhiên, việc sử dụng các thiết bị di động cũng rộng phạm vi dễ bị tổn thương trong các cuộc tấn công, bởi đây là một trong những liên kết yếu nhất trong cơ sở hạ tầng công nghệ thông tin của hầu hết các tổ chức/doanh nghiệp (TC/DN). Việc nhận thức rõ những mối đe dọa về an

toàn đối với thiết bị di động sẽ giúp người dùng (cá nhân và tổ chức) tìm được các biện pháp đảm bảo an ninh an toàn trong môi trường di động.

Nhận diện các mối đe dọa an toàn thiết bị di động

Thực tế cho thấy trong thời gian vừa qua, các cuộc tấn công mạng nhắm vào cá nhân, doanh nghiệp và các tổ chức chính phủ đã gia tăng cả về tần suất và sự tinh vi. Do đó, các mối đe dọa trên các thiết bị di động được đặc biệt quan tâm. Theo một khảo sát trên quy mô toàn cầu về bảo mật trên các thiết bị di động do công ty nghiên cứu thị trường Dimensional Research (Mỹ) thực hiện năm 2017 cho biết, cứ mỗi 10 công ty thì có 2 công ty đã từng bị tấn công trên các thiết bị di động; đáng ngạc nhiên nhất là có tới 24% không biết liệu họ có bị xâm phạm an ninh thông qua các thiết bị di động hay không.

Số lượng phần mềm độc hại tấn công vào các thiết bị di động cũng lớn hơn theo từng ngày, từng giờ với mức độ vô cùng nguy hiểm. Ví dụ, năm 2017, một loại mã độc mang tên CopyCat đã lây nhiễm hơn 14 triệu thiết bị Android trên toàn cầu và đã root thành công khoảng 8 triệu thiết bị di động. Tỷ lệ thành công đạt mức 54% mà gần như không tìm thấy đối với hầu hết các phần mềm độc hại hiện nay. Đầu năm 2018, CrossRAT là một Trojan truy cập từ xa trên nhiều nền tảng, có thể tấn công 4 hệ điều hành phổ biến hiện nay là Windows, Solaris, Linux, và macOS, cho phép kẻ tấn công điều khiển thiết bị từ xa như sử dụng hệ thống tập tin, chụp màn hình, chạy các tập tin thực thi tùy ý và chiếm quyền quản lý hệ thống. Trung tuần tháng 5 vừa qua, công ty công nghệ Securus Technologies (Mỹ) đã rao bán dữ liệu định vị theo thời gian thực của hàng triệu người dùng. Đáng chú ý, Securus Technologies nhận dữ liệu từ một công ty khác có tên là LocationSmart và bản thân công ty LocationSmart cũng mua dữ liệu từ các công ty truyền thông như AT&T, Sprint, T-Mobile và Verizon.

Theo các chuyên gia bảo mật, những vi phạm an toàn thiết bị di động sẽ còn gia tăng trong thời gian tới, tiếp tục khiến cho những nguy cơ mất an toàn thông tin từ chính các thiết bị di động trở nên nguy hiểm hơn. Vì thế ở góc độ người dùng, nhất là các TC/DN cần phải nhận diện được các mối đe dọa đối với thiết bị di động để tận dụng được lợi ích từ thiết bị di động nhưng vẫn đảm bảo vấn đề an toàn cho hoạt động của mình. Cụ thể, các mối đe dọa trên thiết bị di động có thể được chia thành nhiều loại như các mối đe dọa từ vật lý, mạng, hệ thống và ứng dụng:

- ***Các mối đe dọa vật lý***

Một thách thức phải đối mặt trong bảo mật di động là khi thiết bị di động bị đánh mất hoặc bị ăn trộm. Những thiết bị di động bị lọt vào tay của tin tặc sẽ rất nguy hiểm, chúng có thể khai thác những thông tin dữ liệu trên thiết bị. Do đó, người dùng cần phải cất giữ thiết bị di động của mình. Ngoài ra, cần phải mã hóa và xác thực truy nhập cho thiết bị để tránh những truy nhập trái phép.

- ***Các mối đe dọa từ mạng***

Các thiết bị di động thường sử dụng các giao thức mạng không dây phổ biến như Wifi và Bluetooth để kết nối. Mỗi giao thức này đều có các lỗ hổng riêng và dễ bị tấn công bằng cách sử dụng các công cụ sẵn có như Wifite hoặc Aircrack-ng Suite. Do đó, người dùng chỉ nên kết nối với các mạng đáng tin cậy bằng cách sử dụng giao thức WPA2 hoặc các giao thức bảo mật mạng tốt hơn.

- ***Các mối đe dọa từ hệ thống***

Các lỗ hổng trên thiết bị cũng có thể là lỗi từ nhà sản xuất. Ví dụ, bàn phím SwiftKey trong các thiết bị Android của Samsung đã từng được tìm thấy là dễ bị tấn công nghe lén. Tương tự, hệ điều hành iPhone của thiết bị Apple (iOS) cũng được phát hiện có tồn tại các lỗ hổng, mà một trong số đó là "No iOS Zone"; lỗ hổng này cho phép tin tặc làm treo các thiết bị iPhone, iPad hoặc iPod Touch bằng sóng Wifi…

- ***Các mối đe dọa từ ứng dụng***

Tương tự như lỗ hổng hệ thống, các ứng dụng của bên thứ ba trên thiết bị di động cũng có thể lỗi thời. Một số nhà phát triển ứng dụng không phát hành bản cập nhật phần mềm kịp thời hoặc có thể đã giảm hỗ trợ cho các phiên bản hệ điều hành cũ hơn. Sử dụng phần mềm đã lỗi thời làm tăng nguy cơ kẻ tấn công có thể khai thác lỗ hổng liên quan đến phần mềm này.

Những kẻ tấn công thường sử dụng các kỹ thuật xã hội để lừa người dùng cài đặt các ứng dụng độc hại này, có thể qua một liên kết trong tin nhắn, một siêu liên kết rút gọn hoặc một ứng dụng đóng gói lại giả mạo một ứng dụng hợp pháp. Các ứng dụng độc hại có thể thực hiện các hành vi độc hại khi được cài đặt trên thiết bị như lấy cắp dữ liệu, tải xuống phần mềm độc hại hoặc thậm chí điều khiển thiết bị từ xa. Những hành vi này có thể dẫn đến tổn thất về tài chính và các hình thức tổn thất hữu hình hoặc vô hình khác cho cá nhân hoặc tổ chức.

2.2. Nguy cơ mất an toàn đối với thiết bị thông minh

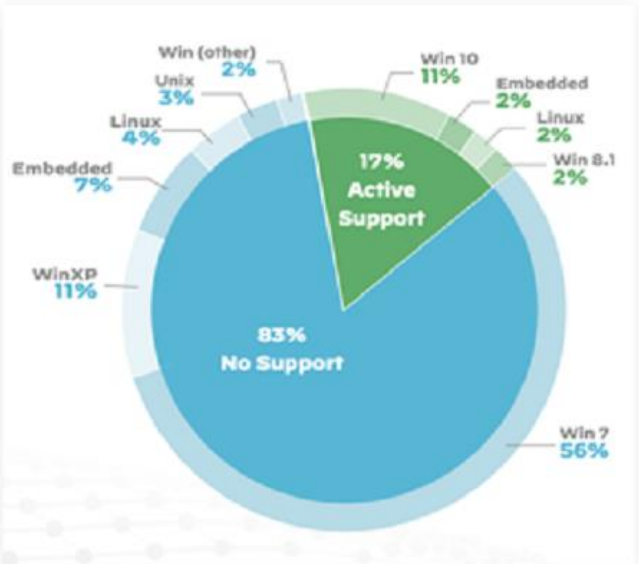
Ngày nay, khi càng nhiều kết nối được thiết lập, sẽ có càng nhiều dữ liệu được ảo hóa và trở thành mục tiêu tấn công của tội phạm công nghệ cao. Vì vậy trong bối cảnh IoT đang trên đà phát triển bùng nổ, nhanh chóng cải thiện năng lực dự báo, phòng ngừa và ứng phó với các lỗ hổng an toàn an ninh thông tin chính là một trong những nhiệm vụ cần thực hiện hàng đầu.

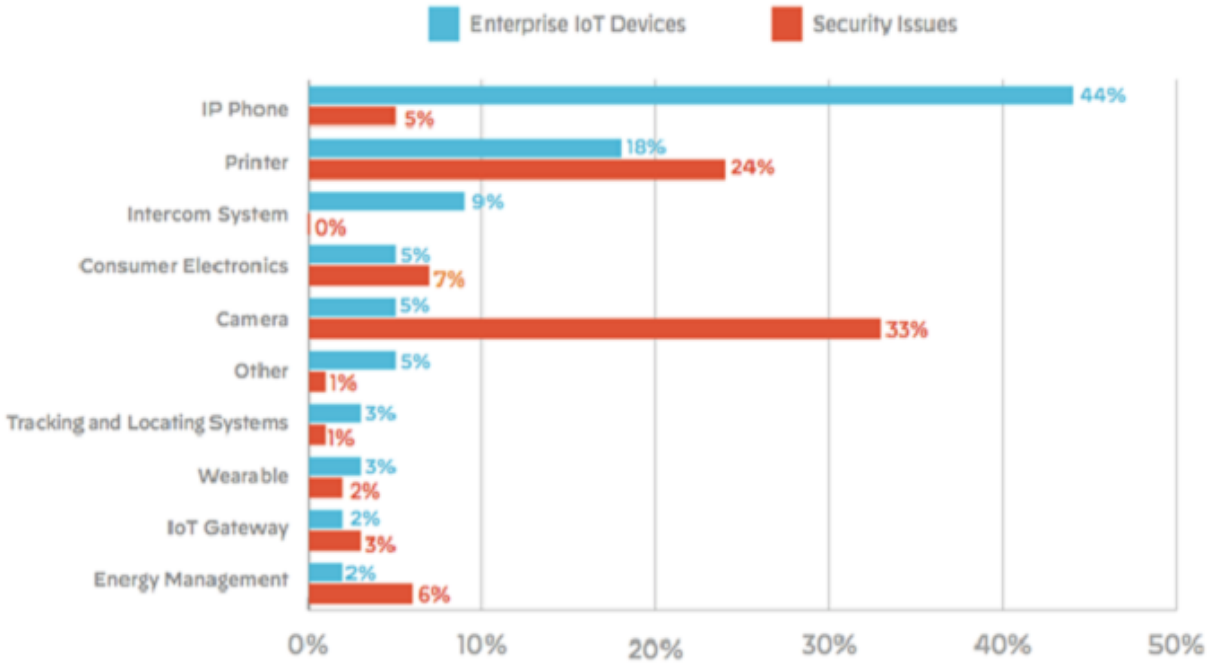
Theo số liệu phân tích được:

- 98% dữ liệu IoT không được mã hóa. Thông qua hình thức nghe lén, hacker có thể dễ dàng thu thập và đọc được các dữ liệu mật được trao đổi giữa các thiết bị trên hệ thống với nhau hoặc giữa chúng với hệ thống quản lý, giám sát.

- 57% các thiết bị IoT trong hệ thống được xem là các rủi ro an toàn thông tin (ATTT) và khởi nguồn cho các cuộc tấn công mạng quy mô vừa và lớn.

- 83% các thiết bị y khoa phục vụ công tác chẩn đoán bằng hình ảnh đang sử dụng các hệ điều hành đã ngừng hỗ trợ từ hãng. Số liệu có sự tăng vọt so với năm 2018, với 56%. Nguyên nhân chính của vấn đề này bắt nguồn từ việc Microsoft đã chính thức khai tử Windows 7 từ đầu năm 2020. Việc tiếp tục sử dụng các thiết bị y tế với hệ điều hành không còn cập nhật các bản vá lỗi có thể dẫn đến các rủi ro lộ lọt thông tin y tế nhạy cảm hoặc gây gián đoạn hoạt động khám chữa bệnh trong trường hợp tin tặc khai thác các lỗ hổng bảo mật trên hệ điều hành. Hình ảnh bên dưới minh họa tỉ lệ các thiết bị y khoa sử dụng các hệ điều hành không còn được cập nhật các bản vá lỗi từ nhà sản xuất.

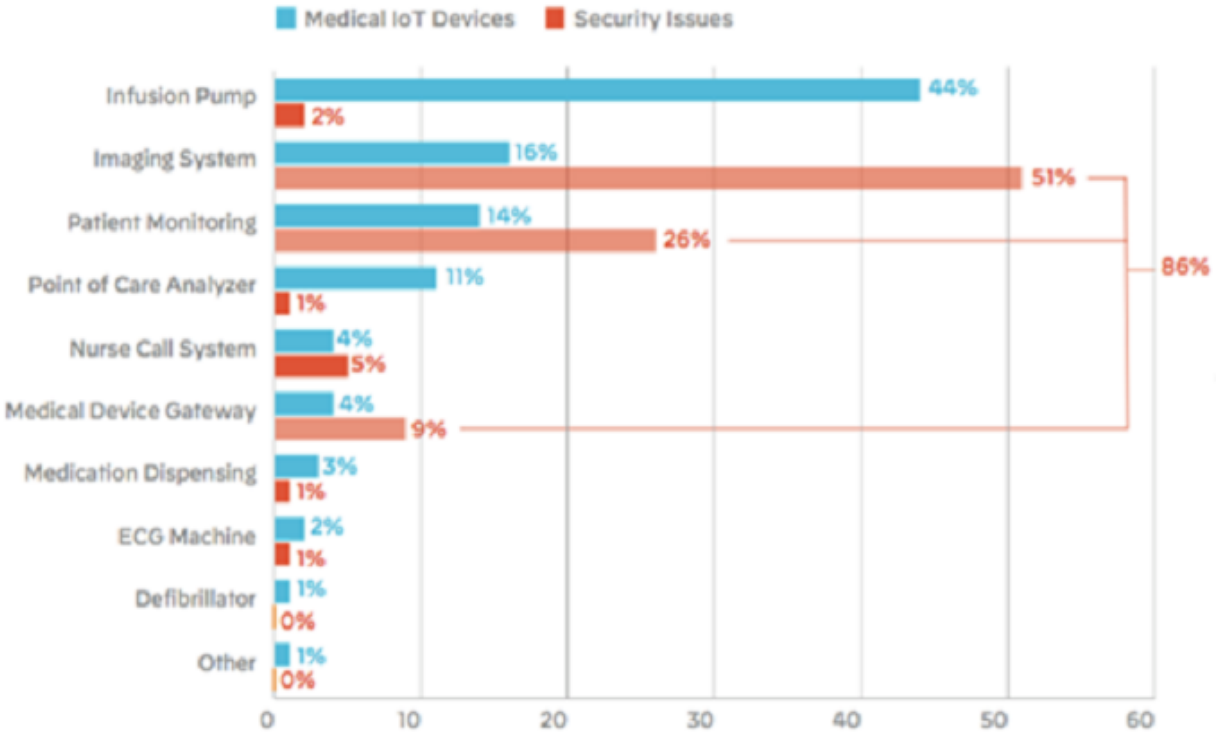




Hình 1. Thống kê về phần trăm số lượng các thiết bị IoT sử dụng và tỉ lệ các mối đe dọa ATTT liên quan đến chúng

Qua biểu đồ trên, có thể thấy rằng IP phone là thiết bị được sử dụng phổ biến nhất, tuy nhiên rủi ro mất an toàn thông tin đối với loại thiết bị này chỉ chiếm 5%. Mặc dù chỉ chiếm 18% và 5% về số lượng các thiết bị trong hệ thống, máy in và camera an ninh lại là hai loại thiết bị tồn tại nhiều vấn đề an toàn bảo mật nhất, với 24% và 33% tương ứng. Năm 2016, gần 600.000 thiết bị CCTV camera đã bị thỏa hiệp và trở thành nạn nhân của mạng lưới botnet Mirai.

Đối với các tổ chức hoạt động trong lĩnh vực y sinh, thiết bị chẩn đoán bằng hình ảnh, máy giám sát sức khỏe bệnh nhân hay thiết bị thu thập dữ liệu y sinh là các thành phần ẩn chứa nhiều rủi ro an toàn thông tin nhất. Số liệu được thể hiện qua biểu đồ bên dưới, với 86% các vấn đề an toàn thông tin của hệ thống liên quan đến các thiết bị này.



Hình 2. Thống kê về phần trăm số lượng các thiết bị IoT sử dụng trong y sinh và tỉ lệ các mối đe dọa ATTT liên quan đến chúng

Một yếu tố khác liên quan đến rủi ro mất ATTT đó là việc quy hoạch các mạng riêng ảo (VLAN) tại các tổ chức khám chữa bệnh chưa được quy hoạch đúng cách và đang sử dụng chung một mạng riêng ảo cho cả thiết bị IoT và thiết bị CNTT chuyên dụng. Chính điều này dẫn đến nguy cơ lây nhiễm virus, phát tán mã độc giữa các thiết bị với nhau. Các thiết bị thuộc hệ thống thông tin trọng yếu như máy chủ, thiết bị định tuyến, tường lửa, trong trường hợp bị lây nhiễm, hoặc bị thỏa hiệp có thể khiến hệ thống mạng của tổ chức bị đánh sập hoàn toàn.

Do tồn tại nhiều điểm yếu, các thiết bị IoT dễ dàng bị kiểm soát bởi hacker. Các thiết bị này được sử dụng làm bàn đạp cho tấn công leo thang vào các thiết bị thông tin trọng yếu của tổ chức. Một trong các điểm yếu phổ biến liên quan đến bảo mật của thiết bị IoT chính là mật khẩu truy cập thiết bị. Nhiều tổ chức không thay đổi và sử dụng chính mật khẩu mặc định của thiết bị, dẫn đến việc các thiết bị này dễ dàng bị khai thác và chiếm quyền do độ mạnh và phức tạp của mật khẩu gần như không có. Qua khảo sát, các thiết bị thuộc một số nhà sản xuất khác nhau sử dụng các mật khẩu mặc định giống nhau, chẳng hạn như p@sswOrd, 123456 hay abc123. Chính điều này làm cho các thiết bị IoT dễ dàng bị tấn công và kiểm soát. Để khắc phục nhược điểm này, trong điều luật SB-327 - California ngày

01/01/2020 có hiệu lực từ đã quy định về việc ngăn cấm sử dụng mật khẩu mặc định với thiết bị IoT có kết nối Internet.

Theo đó, có thể kết luận 5 nguy cơ mất an toàn thông tin lớn nhất đối với IoT – các thiết bị thông minh là: Tồn tại điểm yếu, lỗ hổng trên thiết bị IoT khiến cho tin tặc có thể dễ dàng thâm nhập, tấn công; Mật khẩu mặc định hoặc dễ đoán; Năng lực về an toàn thông tin của nhà sản xuất thiết bị còn hạn chế; Khả năng cập nhật, vá lỗi hạn chế; Nhận thức về an toàn thông tin của người dùng còn chưa cao.

CHƯƠNG 3. CÁC BIỆN PHÁP BẢO VỆ THIẾT BỊ DI ĐỘNG, THIẾT BỊ THÔNG MINH

3.1. Các biện pháp bảo vệ thiết bị di động

Đảm bảo an toàn cho các thiết bị di động là một nhiệm vụ quan trọng, cấp thiết trong kỷ nguyên số, khi mà các nguy cơ tấn công ngày càng gia tăng. Do đó, cần có một giải pháp an toàn được thiết kế có hệ thống, gồm 5 yếu tố chính – Dự báo, Bảo vệ, Phát hiện, Ứng phó và Thực hành. Cụ thể:

- ***Dự báo***

Dự báo về các cuộc tấn công với các yếu tố như hướng tấn công, mức độ gây hại và hậu quả của nó là vô cùng quan trọng. Vì thế, việc chủ động theo dõi, giám sát không gian mạng sẽ giúp các tổ chức có được những thông báo về các mối đe dọa mới có thể ảnh hưởng đến an ninh an toàn, từ đó đưa ra các xem xét, đánh giá hệ thống của mình sẽ chịu những tác động gì để chủ động xây dựng các biện pháp bảo vệ thích hợp.

- ***Bảo vệ***

Bảo vệ là một yếu tố quan trọng của giải pháp bảo mật di động, bao gồm hai khía cạnh chính. Khía cạnh đầu tiên là ngăn chặn các mối đe dọa không mong muốn xâm nhập hoặc ảnh hưởng đến hệ thống di động. Ví dụ, phần mềm độc hại có thể tồn tại dưới dạng gói hoặc tệp ứng dụng. Vì thế, thực hiện quét lưu lượng đến tại proxy mạng hoặc cổng để kiểm tra lưu lượng độc hại trước khi chuyển tiếp tới thiết bị, hay cập nhật kịp thời cho các ứng dụng và hệ điều hành của các thiết bị để vá bất kỳ lỗ hổng nào là những biện pháp bảo vệ khỏi ứng dụng độc hại.

Khía cạnh bảo vệ khác là bảo vệ dữ liệu nhạy cảm để tránh bị rò rỉ tới các điểm đích không được cho phép. Điều này có thể thực hiện được bằng cách sử

dụng mạng riêng ảo và tường lửa để chặn lưu lượng gửi đến các đích không được cho phép.

- ***Phát hiện***

Phần mềm độc hại là một trong những công cụ chính được sử dụng bởi kẻ tấn công để thực hiện các hoạt động độc hại trên thiết bị di động. Việc phát hiện sớm các phần mềm độc hại có thể làm giảm tác hại và hạn chế sự lây lan. Việc sử dụng các phần mềm chống virus cũng sẽ giúp phát hiện các phần mềm độc hại. Tuy nhiên, do các cuộc tấn công bằng phần mềm độc hại ngày càng tinh vi hơn, vì thế cần một phương pháp mới sử dụng kết hợp phân tích tĩnh và động, cũng như kỹ thuật học máy để đạt được kết quả toàn diện.

Một phương pháp phát hiện khác là theo dõi và thu gom các hoạt động và hành vi bất thường của hệ thống. Sau khi phát hiện bất thường, cảnh báo được kích hoạt cho người dùng và hệ thống báo cáo phụ trợ. Các cảnh báo này có thể cung cấp thông tin về các hoạt động độc hại và có thể tương quan với các dữ liệu bảo mật khác để cung cấp thông tin hữu ích giúp phát hiện và phản hồi các mối đe dọa nhanh chóng.

- ***Ứng phó***

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

Vì thế, ứng phó với sự cố an ninh mạng là một yếu tố quan trọng trong bất kỳ khung an ninh, an toàn nào. Khi xảy ra sự cố, nhóm ứng phó sự cố cần phải lập tức khoanh vùng, hạn chế thiệt hại sự cố và cô lập các hệ thống bị ảnh hưởng để ngăn chặn hệ thống bị thiệt hại thêm. Sau đó mới tiến hành tìm nguồn tốc tấn công và xây dựng hệ thống phòng chống để ngăn chặn sự cố tương tự xảy ra; Phục hồi các hệ thống bị ảnh hưởng, đảm bảo không có mối đe dọa liên quan tới vấn đề an ninh mạng tồn đọng. Ví dụ trong một cuộc tấn công dựa trên ứng dụng, thì ứng dụng đó sẽ được phân tích để hiểu hành vi gây hại và các thông tin quan trọng khác của ứng dụng để đánh giá tác động và tìm các biện pháp đối phó thích hợp.

- ***Thực hành***

Mặc dù người dùng có thể nhận thức được rằng thiết bị di động là một mục tiêu dễ tấn công, nhưng ít người nghĩ rằng mình sẽ trở thành nạn nhân của các cuộc tấn công này. Do đó, điều quan trọng là phải hướng dẫn, phổ biến, thực hành và tập huấn cho người dùng về các phương pháp an toàn khi sử dụng thiết bị di động và cập nhật cho họ về các hình thức tấn công mới.

Đối với đội ngũ chuyên trách về công nghệ thông tin, cần được diễn tập xử lý tấn công mạng thường xuyên, vì đây là cơ hội để thảo luận, chia sẻ kinh nghiệm, thông tin, rèn luyện, phối hợp, nâng cao khả năng sẵn sàng ứng phó với các cuộc tấn công mạng, bảo vệ hệ thống mạng, hạ tầng thông tin quan trọng.

Để việc bảo mật di động đi trước các mối đe dọa mạng tinh vi trên thiết bị di động, thì giải pháp bảo mật di động cần được xây dựng một cách có hệ thống, toàn diện. Khi có sự cố về an ninh mạng, việc chia sẻ thông tin, giải pháp khắc phục sự cố và xử lý tình huống là rất quan trọng. Để xử lý tốt các sự cố, cần xây dựng càng nhiều kịch bản tấn công càng tốt và chủ động xử lý theo kịch bản khi xảy ra sự cố thật.

Ngoài ra, cần chú ý rằng bảo mật di động là một quá trình phòng thủ theo chiều sâu bao gồm các khâu phát triển, vận hành, xây dựng cơ sở hạ tầng bảo vệ tốt và có một đội ngũ chuyên trách vấn đề bảo mật riêng cho các thiết bị di động.

Có nhiều ứng dụng và công cụ hỗ trợ bảo mật cho thiết bị di động, giúp người dùng và tổ chức duy trì môi trường an toàn cho dữ liệu và thông tin cá nhân. Dưới đây là một số ứng dụng và công cụ phổ biến:

1. Phần mềm diệt virus và bảo mật: giúp bảo vệ thiết bị di động của bạn khỏi malware, virus và các mối đe dọa an ninh khác.

- Avast Mobile Security: Bảo vệ di động khỏi virus, malware, và cung cấp tính năng anti-theft.

- McAfee Mobile Security: Quét virus, bảo vệ quyền riêng tư, và giúp quản lý ứng dụng.

- Bitdefender Mobile Security, Kaspersky Mobile Antivirus, Norton Mobile Security, AVG AntiVirus for Android, Trend Micro Mobile Security, Sophos Intercept X for Mobile…

Tuy nhiên, đối với mọi ứng dụng bảo mật, quan trọng nhất là cập nhật định kỳ để đảm bảo tính hiệu quả và bảo mật tốt nhất. Sự chọn lựa giữa các ứng dụng

cụ thể có thể phụ thuộc vào nhu cầu cụ thể của người dùng và các tính năng đặc biệt mà người dùng muốn.

2. Mạng riêng ảo (VPN): giúp bảo vệ dữ liệu cá nhân, VPN mã hóa dữ liệu giữa thiết bị di động của bạn và máy chủ VPN, ngăn chặn người xem không mong muốn từ theo dõi và thu thập dữ liệu cá nhân của bạn. Khi kết nối với mạng Wi-Fi công cộng, VPN giúp bảo vệ dữ liệu của bạn khỏi nguy cơ bị đánh cắp hoặc tấn công từ những người sử dụng cùng mạng. VPN cho phép bạn truy cập nội dung trực tuyến mà có thể bị giới hạn địa lý, như các dịch vụ streaming hoặc trang web. Khi bạn kết nối với mạng từ xa, VPN tạo một kênh an toàn giữa thiết bị của bạn và mạng mục tiêu, ngăn chặn nguy cơ tấn công từ phía mạng Internet.

- ExpressVPN: Cung cấp kết nối VPN an toàn, giúp bảo vệ dữ liệu khi sử dụng Wi-Fi công cộng.

- NordVPN: Bảo vệ quyền riêng tư trực tuyến bằng cách ẩn địa chỉ IP và mã hóa kết nối Internet.

3. Ứng dụng quản lý mật khẩu: giúp bảo vệ thông tin đăng nhập và tăng cường an ninh cho thiết bị di động của bạn.

- LastPass: Lưu trữ mật khẩu an toàn và tạo mật khẩu mạnh tự động.

- 1Password: Quản lý và bảo vệ mật khẩu, thông tin thẻ tín dụng và ghi chú an toàn.

- Dashlane, Keeper, Bitwarden, NordPass, Enpass,…

Chọn ứng dụng quản lý mật khẩu dựa trên nhu cầu cụ thể của người dùng, chẳng hạn như tích hợp với các nền tảng cụ thể, tính năng bảo mật, hoặc tính tương thích với các dịch vụ khác. Người dùng nên chọn một mật khẩu chính mạnh và duy trì an toàn để truy cập ứng dụng quản lý mật khẩu của mình, thường xuyên sao lưu dữ liệu quản lý mật khẩu và kiểm tra tính tương thích với các thiết bị và trình duyệt khác nhau.

4. Ứng dụng quản lý thiết bị và theo dõi:

- Find My iPhone (iOS) / Find My Device (Android): Theo dõi vị trí thiết bị và cung cấp tính năng khoá từ xa.

- Cerberus (Android): Theo dõi, khoá, và xoá dữ liệu từ xa trên thiết bị Android.

5. Ứng dụng mã hóa dữ liệu:

- Signal: Ứng dụng nhắn tin có mã hóa end-to-end, đảm bảo sự an toàn cho nội dung tin nhắn.

- VeraCrypt (Android): Mã hóa và bảo vệ dữ liệu trên thiết bị di động.

- Cryptomator: Tạo "hộp treo" (vault) mã hóa trên các dịch vụ lưu trữ đám mây như Google Drive hoặc Dropbox, mã hóa file và thư mục.

- AES Crypt: Mã hóa tệp tin đơn giản sử dụng AES-256, hỗ trợ trên nhiều nền tảng, bao gồm cả iOS và Android.

- Boxcryptor: Mã hóa dữ liệu lưu trữ trên các dịch vụ đám mây như Google Drive, OneDrive, Dropbox, hỗ trợ nhiều nền tảng, bao gồm cả di động.

- Tresorit: Mã hóa dữ liệu và file trên dịch vụ đám mây, theo dõi và ghi lại mọi sự thay đổi trên file.

- FileVault (iOS): Tính năng được tích hợp sẵn trong iOS để mã hóa dữ liệu trên iPhone và iPad, mã hóa tất cả các dữ liệu trên thiết bị.

- Folder Lock: Mã hóa file, thư mục và ổ đĩa, tính năng ẩn và bảo vệ file.

- Encrypto: Mã hóa file để chia sẻ qua email hoặc các phương tiện truyền thông xã hội, dễ sử dụng và tích hợp với nhiều dịch vụ.

- Secrecy: Mã hóa dữ liệu và thông tin cá nhân trên thiết bị Android, bảo vệ ảnh, video, và các tệp tin cá nhân khác.

Trước khi sử dụng ứng dụng mã hóa, đảm bảo rằng người dùng hiểu rõ cách chúng hoạt động và cách quản lý khóa mật khẩu, luôn giữ mã PIN hoặc mật khẩu của bạn an toàn và không chia sẻ chúng với người khác, thường xuyên sao lưu khóa và thông tin quan trọng để tránh mất mát dữ liệu trong trường hợp không mong muốn.

6. Ứng dụng chống Phishing và bảo mật email:

- Lookout: Bảo vệ khỏi phishing và malware thông qua quét email và các tệp đính kèm.

- Microsoft Defender for Office 365 (iOS/Android): Bảo vệ email và tệp đính kèm khỏi malware và email lừa đảo.

7. Ứng dụng bảo vệ dữ liệu cá nhân:

- MyPermissions: Kiểm soát quyền truy cập ứng dụng và dịch vụ khác nhau, đảm bảo quyền riêng tư.

- DuckDuckGo Privacy Browser: Trình duyệt tăng cường quyền riêng tư với tính năng chặn theo dõi và bảo vệ thông tin người dùng.

8. Ứng dụng quản lý quyền riêng tư:

- Norton App Lock: Khoá ứng dụng cụ thể bằng mật khẩu hoặc vân tay để bảo vệ quyền riêng tư.

- Privacy Guard (Android): Kiểm soát quyền truy cập ứng dụng và dữ liệu trên thiết bị Android.

9. Ứng dụng kiểm tra an ninh Wifi:

- WiFi Guard (iOS): Kiểm tra và bảo vệ mạng Wi-Fi khỏi các nguy cơ bảo mật.

- Network Analyzer (Android): Xác định vấn đề bảo mật và quản lý mạng Wi-Fi.

10. Ứng Dụng Quản Lý Công Nghiệp (Doanh Nghiệp):

- MobileIron: Quản lý và bảo mật thiết bị di động trong môi trường doanh nghiệp.

- Microsoft Intune: Cung cấp giải pháp quản lý thiết bị và ứng dụng cho doanh nghiệp.

3.2. Các biện pháp bảo vệ thiết bị thông minh

Để có thể giảm thiểu các rủi ro ATTT, nhìn chung có 4 bước thực tổng quát sau đây:

- ***Nhận biết được các mối de dọa***

Tuy các thiết bị IoT chiếm số lượng gần 30% các thiết bị kết nối mạng trong doanh nghiệp, nhiều tổ chức vẫn chưa nhận thức được các nguy cơ mất ATTT từ loại thiết bị này. Do đó quá trình rà quét và phân loại các thiết bị này là cần thiết và cấp bách để giảm rủi ro cho doanh nghiệp.

Việc phân loại cần thực hiện chia tách các thiết bị IoT thành các nhóm đối tượng khác nhau, ví dụ nhóm đối tượng có kết nối Internet và đối tượng chỉ có kết nối với hệ thống mạng của doanh nghiệp, không có bất cứ kết nối nào ra bên ngoài. Nhóm thiết bị có kết nối Internet cần được áp dụng các chính sách ATTT chặt chẽ hơn, do chúng thuộc nhóm dễ bị hacker khai thác nhất. Thêm vào đó, cần thực hiện quy hoạch riêng VLAN hoặc vùng mạng cho nhóm đối tượng này để tránh lây nhiễm với các thiết bị thuộc hệ thống khác. Có như vậy, việc xử lý và ứng cứu sự cố an ninh thông tin mới diễn ra được thuận lợi do đã có quy hoạch, khoanh vùng các nhóm rõ ràng.

- ***Kiểm soát chặt chẽ các thiết bị có nguy cơ lây nhiễm cao***

Như đã phân tích ở phần trên, một số thiết bị y sinh hay camera an ninh là các thiết bị IoT dễ bị tấn công, khai thác nhất. Do đó các chính sách ATTT đối với loại thiết bị này cần được xem xét kỹ. Chẳng hạn như mật khẩu sử dụng truy cập nghiêm cấm sử dụng mật khẩu mặc định. Bằng chứng là nhiều cuộc tấn công mạng quy mô lớn đã khai thác lỗ hổng bảo mật này, thực hiện rà quét dựa trên tập hợp các mật khẩu mặc định, và biến chúng thành đối tượng của mạng lưới botnet. Ngoài ra, việc cập nhật các bản vá lỗi, các phiên bản hệ điều hành mới cho các thiết bị này cũng là nhiệm vụ thiết yếu hàng đầu trong giảm thiểu rủi ro mất ATTT.

- ***Xây dựng phương án quy hoạch mạng riêng (VLAN) cho các thiết bị IoT***

Với số liệu ghi nhận về việc gia tăng số lượng mạng riêng ảo (VLAN) trong các doanh nghiệp trong hai năm 2018, 2019, việc sử dụng các mạng riêng ảo hoặc quy hoạch cùng dãi mạng cho các thiết bị IoT và các thiết bị CNTT trọng yếu cần được loại bỏ trong thiết kế hệ thống. Xét về mức độ bảo mật và tầm quan trọng cần được bảo vệ, các thiết bị CNTT trọng yếu như máy chủ dịch vụ, thiết bị định tuyến, chuyển mạch,… có mức ưu tiên cao hơn thiết bị IoT. Do đó người quản trị cần xác định, quy hoạch các phân lớp mạng riêng cho hai nhóm thiết bị này. Tùy theo mức ưu tiên, chỉ cho phép truy cập từ thiết bị thuộc vùng có mức bảo mật cao đến các thiết bị thuộc vùng có mức bảo mật thấp hơn, chiều ngược lại sẽ bị chặn. Nếu thực hiện như vậy, trong trường hợp rủi ro, hacker tấn công và kiểm soát được các thiết bị IoT cũng không thể tấn công leo thang đến các thiết bị CNTT trọng yếu, do đã bị chặn bởi thiết bị kiểm soát truy cập.

- ***Xây dựng các hệ thống giám sát***

Để phát hiện và có phương án ứng phó kịp thời, việc xây dựng các hệ thống giám sát ATTT là vô cùng cần thiết. Đối với các hệ thống lớn, việc giám sát được thực hiện trên hai hệ thống là NOC (dùng cho giám sát dịch vụ mạng) và SOC (dùng cho giám sát ATTT). Với các hệ thống nhỏ hơn, việc giám sát dù không phân định rõ giữa NOC và SOC cũng cần có phương án giám sát ATTT. Bởi nhờ vào quá trình giám sát 24/7 và đưa ra các cảnh báo khi có bất thường xảy ra trong hệ thống, việc đề xuất các biện pháp phòng thủ cũng như quá trình truy vết dựa trên log sự kiện hệ thống cũng dễ dàng hơn.

Để nâng cao tính sẵn sàng của hệ thống trước các cuộc tấn công mạng, thiết bị IoT là nhóm đối tượng cần được xem xét kỹ khi ban hành và thực thi các chính sách liên quan đến an toàn thông tin.

Bên cạnh đó, Cục An toàn thông tin đưa ra các giải pháp khắc phục cho 5 nhóm đối tượng chính trong công tác bảo mật IoT: Cơ quan quản lý nhà nước; Nhà sản xuất và phát triển giải pháp cho thiết bị IoT; Doanh nghiệp cung cấp hạ tầng mạng viễn thông và Internet; Doanh nghiệp cung cấp sản phẩm, dịch vụ an toàn thông tin; Người sử dụng thiết bị IoT. Cụ thể:

- ***Đối với cơ quan quản lý nhà nước***

Cần xây dựng chiến lược quốc gia phát triển nền tảng, đảm bảo an toàn, an ninh mạng cho IoT; Xây dựng hành lang pháp lý theo hướng tiêu chuẩn, quy chuẩn hóa và thực thi kiểm định; Có cơ chế khuyến khích, hỗ trợ phát triển sản phẩm, dịch vụ an toàn thông tin, khởi nghiệp cho IoT; Tập trung đào tạo nguồn nhân lực phát triển IoT; Chú trọng tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin IoT.

- ***Đối với nhà sản xuất và phát triển IoT***

Cần tuân thủ tiêu chuẩn, quy chuẩn khi sản xuất thiết bị IoT; Bắt buộc người sử dụng thay đổi mật khẩu mặc định; Tự động hóa việc cập nhật phần mềm, gói bảo mật mà không cần người dùng phải thực hiện thủ công; Coi an toàn thông tin cho thiết bị IoT là lợi thế cạnh tranh.

- ***Đối với doanh nghiệp viễn thông, Internet***

Thực hiện giám sát, ngăn chặn các máy chủ điều khiển mã độc IoT; Hỗ trợ khách hàng rà quét, bóc gỡ mã độc IoT; Kiểm định thiết bị IoT trước khi kết nối mạng.

- ***Đối với người sử dụng hoặc tổ chức***

Cân nhắc khi mua sắm thiết bị IoT, lựa chọn sản phẩm của các nhà sản xuất uy tín; Thay đổi mật khẩu, cấu hình mặc định; Đặt các thiết bị IoT trong vùng mạng cách ly; Thiết lập quy trình cập nhật cho thiết bị IoT hoặc thay thế nếu bắt buộc.

- ***Đối với doanh nghiệp cung cấp sản phẩm, dịch vụ an toàn thông tin:***

Nghiên cứu, phát triển và cung cấp sản phẩm, dịch vụ an toàn thông tin cho IoT; Hợp tác với nhà sản xuất thiết bị IoT hoặc nhà mạng viễn thông, Internet để triển khai giải pháp sản phẩm, dịch vụ an toàn thông tin./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG