BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ CÁC NGUY CƠ MẤT AN TOÀN THÔNG TIN"

Hà Nội, năm 2023

1. TỔNG QUAN

Tháng 6/2023, Bộ Thông tin và Truyền thông đã cảnh báo, hướng dẫn xử lý 1.723 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam, nâng số sự cố tấn công mạng vào hệ thống trong nước 6 tháng đầu năm 2023 lên 6.362 cuộc.

Đánh giá tình hình thực hiện Nghị quyết số 17/NQ-CP của Chính phủ về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử Quý II năm 2023, Bộ Thông tin và Truyền thông, cơ quan thường trực Ủy ban quốc gia về chuyển đổi số, nhận định: Việc tổ chức kiểm tra, đánh giá, giám sát, bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin phục vụ Chính phủ điện tử tiếp tục được đẩy mạnh thời gian qua.

Cụ thể, trong tháng 6 vừa qua, Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận, cảnh báo và hướng dẫn xử lý 1.723 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam, tăng gần 2,5 lần so với tháng 5/2023, tăng 46,3% so với cùng kỳ tháng 6 năm ngoái.

Tuy nhiên, lũy kế trong nửa đầu năm nay, Cục An toàn thông tin đã ghi nhận, cảnh báo và hướng dẫn xử lý 6.362 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam, giảm 4,2% so với 6 tháng đầu năm 2022.

Với quan điểm xây dựng Chính phủ điện tử gắn kết chặt chẽ với bảo đảm an toàn thông tin, an ninh mạng, an ninh quốc gia, bảo vệ thông tin cá nhân, thời gian tới, Bộ Thông tin và Truyền thông vẫn tiếp tục tăng cường giám sát an toàn hệ thống thông tin, chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê và tiếp tục đẩy mạnh tuyên truyền, cảnh báo trên các phương tiện thông tin đại chúng để người dùng biết, phòng tránh. Cùng với đó, Bộ Thông tin và Truyền thông cũng tiếp tục có các văn bản cảnh báo cho các bộ, ngành, địa phương và các thành viên trong mạng lưới ứng cứu sự cố để đôn đốc việc rà soát điểm yếu lỗ hổng, dấu hiệu tấn công mạng.

2. CÁC KHÁI NIỆM VỀ AN TOÀN THÔNG TIN MẠNG

Theo quy định tại Khoản 1, Điều 3, Luật an toàn thông tin mạng năm 2015, An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoạt trái phép, với mục đích đảm bảo tính nguyên vẹn, bảo mật và khả dụng của thông tin.

Bên cạnh đó, An toàn thông tin theo quy định tại Khoản 2, Điều 3, Nghị định 64/2007/NĐ-CP bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật với hệ thống thông tin nhằm mục đích bảo vệ, khôi phục các hệ thống, dịch vụ và nội dung thông tin với các nguy cơ tự của tự nhiên hoặc do con người gây ra.

Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin giúp đảm bảo cho hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn, thông tin bao gồm các nội dung bảo vệ, bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng. Trong đó "Mạng" là môi trường trong đó thông tin sẽ được truyền đi, thu thập và xử lý, lưu trữ, trao đổi thông qua mạng viễn thông và mạng máy tính.

3. CHÍNH SÁCH VÀ QUY ĐỊNH PHÁP LUẬT VỀ AN TOÀN THÔNG TIN MẠNG

Chính sách của Nhà nước về an toàn thông tin mạng được quy định tại Điều 5 Luật An toàn thông tin mạng 2015. Cụ thể có các nội dung như sau:

"1. Đẩy mạnh đào tạo, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng, kỹ thuật an toàn thông tin mạng đáp ứng yêu cầu ổn định chính trị, phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội.

2. Khuyến khích nghiên cứu, phát triển, áp dụng biện pháp kỹ thuật, công nghệ, hỗ trợ xuất khẩu, mở rộng thị trường cho sản phẩm, dịch vụ an toàn thông tin mạng do tổ chức, cá nhân trong nước sản xuất, cung cấp; tạo điều kiện nhập khẩu sản phẩm, công nghệ hiện đại mà tổ chức, cá nhân trong nước chưa có năng lực sản xuất, cung cấp.

3. Bảo đảm môi trường cạnh tranh lành mạnh trong hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; khuyến khích, tạo điều kiện cho tổ chức, cá nhân tham gia đầu tư, nghiên cứu, phát triển và cung cấp sản phẩm, dịch vụ an toàn thông tin mạng.

4. Nhà nước bố trí kinh phí để bảo đảm an toàn thông tin mạng của cơ quan nhà nước và an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.".

Chính sách của Nhà nước về nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng 2015. Cụ thể có các nội dung như sau:

"1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng

quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.".

Chính sách của Nhà nước về các hành vi bị nghiêm cấm trong vấn đề an toàn thông tin mạng được quy định tại Điều 7 Luật An toàn thông tin mạng 2015. Cụ thể có các nội dung như sau:

"1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.".

Quy định của Nhà nước về xử lý vi phạm pháp luật về an toàn thông tin mạng được quy định tại Điều 8 Luật An toàn thông tin mạng 2015, cụ thể: "Người

nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.”.

Bộ Thông tin và Truyền thông có quyết định phê duyệt Chương trình bồi dưỡng, tập huấn kiến thức, kỹ năng số và an toàn thông tin cho cán bộ, công chức các xã thuộc Chương trình mục tiêu quốc gia xây dựng nông thôn mới giai đoạn 2021 – 2025 tại Quyết định số 1817/QĐ-BTTTT ngày 21/9/2023.

4. CÁC HÌNH THỨC TẤN CÔNG MẠNG VÀ CÁC MỐI ĐE DỌA TRÊN KHÔNG GIAN MẠNG

4.1. Tấn công mạng là gì?

Hiện nay, với thời buổi 4.0, khi công nghệ lên ngôi, là điều kiện thuận lợi để các tội phạm cộng nghệ xuất hiện và phát triển ngày một mạnh mẽ. Trong đó, tấn công mạng là hành vi trái phép tiêu biểu khi nhắc về loại tội phạm này.

Tấn công mạng (cyber attack) là cuộc tấn công trái phép đối với các tài sản digital bên trong mạng của 1 tổ chức do tội phạm mạng (hacker) thực hiện bằng cách sử dụng một hoặc nhiều máy tính chống lại một hoặc nhiều máy tính hoặc mạng. Một cuộc tấn công mạng có thể vô hiệu hóa máy tính, đánh cắp dữ liệu nhằm đặt được các mục tiêu khác nhau mang đến nhiều nguy hiểm và các mối đe dọa vô cùng lớn.

"Tấn công mạng" được hiểu theo 2 nghĩa: hiểu theo nghĩa tích cực (positive way) và hiểu theo nghĩa tiêu cực (negative way):

- Theo nghĩa tích cực (positive way): theo nghĩa hiểu này thì tấn công mạng là việc hacker mũ trắng xâm nhập vào một hệ thống mạng, thiết bị hay website để kiểm tra và tìm ra các lỗ hổng bảo mật, tìm kiếm các rủi ro tấn công nhằm bảo vệ các thông tin lưu trữ của tổ chức, doanh nghiệp giúp ngăn chặn sự đe dọa với ý đồ xấu từ các hacker.

- Theo nghĩa tiêu cực (negative way): tấn công mạng theo nghĩa tiêu cực là hành vi trái pháp luật được thực hiện bởi các hacker mũ đen. Các hacker này sẽ tấn công vào một hệ thống mạng, thiết bị hay website để khai thác các thông tin và tài liệu bí mật của tổ chức, doanh nghiệp hoặc xâm nhập vào các thiết bị cá nhân với các mục đích xấu xa như thay đổi, phá hoại hoặc tống tiền nạn nhân. Tùy vào mức độ nghiệm trọng của những hành vi này sẽ dẫn đến những hệ lụy vô cùng

lớn, ảnh hưởng đến cuộc sống và đời tư của các nạn nhân và các tổn thất vô cùng lớn cho tổ chức, doanh nghiệp bị hại.

4.2. Đối tượng phổ biến bị tấn công mạng

Bất cứ ai có thông tin riêng tư, bí mật được lưu trữ trên môi trường mạng đều có thể trở thành đối tượng bị tấn công. Các đối tượng phổ biến bị tấn công mạng là các cá nhân, doanh nghiệp tư nhân và tổ chức chính phủ hoặc phi chính phủ. Các hacker sẽ tiếp cận nhưng đối tượng này qua mạng nội bộ như máy tính hay thiết bị điện tử, hoặc tiếp cận qua con người nhờ các thiết bị di động, mạng social và các ứng dụng phần mềm nhằm đe dọa, làm ảnh hưởng tới đời sống, tinh thần của cá nhân hoặc đe dọa đến các thông tin nội bộ làm ảnh hưởng đến hiệu quả hoạt động của doanh nghiệp hay các phần tử chống phá nhà nước muốn lật đổ chính quyền.

4.3. Các hình thức tấn công mạng phổ biến

a) Malware – Tấn công bằng phần mềm độc hại

Khái niệm: Malware (hay phần mềm độc hại) là thuật ngữ mô tả các chương trình hoặc mã độc có khả năng cản trở hoạt động bình thường của hệ thống bằng cách xâm nhập, kiểm soát, làm hỏng hoặc vô hiệu hóa hệ thống mạng, máy tính, máy tính bảng và thiết bị di động,…

Khi thiết bị nhiễm Malware, bạn có thể nhận thấy các dấu hiệu sau:

- Máy tính chạy chậm, tốc độ xử lý của hệ điều hành giảm cho dù bạn đang điều hướng Internet hay chỉ sử dụng các ứng dụng cục bộ.

- Bạn bị làm phiền bởi quảng cáo pop-up, mà cụ thể hơn là Adware.

- Hệ thống liên tục gặp sự cố, bị đóng băng hoặc hiển thị BSOD – màn hình xanh (đối với Windows).

- Dung lượng ổ cứng giảm bất thường.

- Hoạt động Internet của hệ thống tăng cao không rõ nguyên nhân.

- Tài nguyên hệ thống tiêu hao bất thường, quạt máy tính hoạt động hết công suất.

- Trang chủ của trình duyệt mặc định thay đổi mà không có sự cho phép của bạn. Các liên kết bạn nhấp vào sẽ chuyển hướng bạn đến các trang không mong muốn.

- Các thanh công cụ, tiện ích mở rộng hoặc plugin mới được thêm vào trình duyệt.

- Các chương trình anti-virus ngừng hoạt động và không cập nhật được.

- Bạn nhận được thông báo đòi tiền chuộc từ Malware, nếu không dữ liệu của bạn sẽ bị xóa.

Cơ chế hoạt động của Malware: Trong quá trình sử dụng Internet, những thao tác sau có thể khiến bạn bị nhiễm Malware:

- Truy cập các trang web độc hại, tải trò chơi, file nhạc nhiễm Malware, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm email độc hại hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật.

- Tải nhầm các ứng dụng độc hại ngụy trang dưới dạng các ứng dụng hợp pháp, các thông báo cảnh báo khi cài đặt ứng dụng, đặc biệt khi ứng dụng yêu cầu quyền truy cập email hoặc thông tin cá nhân.

- Tải ứng dụng ở các nguồn không đáng tin cậy.

- Vô tình cài đặt các phần mềm bổ sung đi kèm với ứng dụng chứa Malware.

- Ngoài ra, việc không sử dụng các chương trình bảo mật cũng là lý do khiến Malware xâm nhập dễ dàng hơn.

Các loại Malware phổ biến:

Virus

Loại chương trình này vô cùng nguy hiểm vì có khả năng sinh sôi, lây lan ra khắp hệ thống phần mềm, gây thiệt hại phần cứng,… với tốc độ rất nhanh. Nếu không khắc phục kịp thời, mọi thông tin, dữ liệu, thậm chí là thiết bị đều sẽ mất kiểm soát.

Worm

Hay còn được hiểu với nghĩa là con sâu và chương trình này còn độc hại hơn cả virus. Bởi Worm có thể tự sinh sôi, hoạt động mà không chịu bất kỳ sự tác động, điều khiển nào đến từ con người cả. Thậm chỉ khi đã bị "tiêu diệt" rồi thì vẫn có khả năng tự tái tạo, hoạt động lại như bình thường. Nghe khá giống với kiểu AI – trí tuệ nhân tạo.

Trojan

Một phần mềm được xây dựng như một chương trình chính chủ, hợp pháp và uy tín. Được quảng cáo và sở hữu chức năng bảo vệ, giúp máy tính tránh khỏi sự xâm nhập, tấn công của Virus. Thực chất Trojan giống như một cánh cổng mở ra và cho phép hàng triệu loại Virus khác nhau tiến công, gây hại cho máy tính. Mặc dù Trojan không có chức năng sao chép dữ liệu những lại có khả năng "hủy diệt" rất kinh khủng.

Spyware

Spyware hoàn toàn không có chức năng hủy hoại dữ liệu nhưng lại là chuyên gia theo dõi, sao chép và quan sát hoạt động của người dùng. Bất kỳ dữ liệu nào được nhập, xuất ra khỏi thiết bị đều được Spyware ghi nhận, cung cấp lại cho những kẻ gian mà không ai hay biết.

Rootkit

Kể từ khi người dùng cài đặt phần mềm này vào thiết bị, Rootkit ngay lập tức tấn công và tước quyền quản trị. Khi này các tin tắc có thể tự do truy cập trái phép, vượt qua được bất cứ "bức tường bảo vệ" nào một cách dễ dàng. Đánh cấp dữ liệu, theo dõi hành vi người dùng một cách ung dung mà không có bất kỳ cảnh báo lỗi hệ thống nào diễn ra.

Ransomware

Ngăn bạn truy cập vào thiết bị và mã hóa dữ liệu, sau đó buộc bạn phải trả tiền chuộc để lấy lại chúng. Ransomware được xem là vũ khí của tội phạm mạng vì nó thường dùng các phương thức thanh toán nhanh chóng bằng tiền điện tử.

Cách phòng tránh Malware:

- Bạn nên cảnh giác với các web có domain kết thúc bằng tập hợp các chữ cái riêng lẻ, và có đuôi không giống như bình thường (.com, .vn hay .org,...).

- Bạn nên chú ý đến các dấu hiệu nhiễm Malware của máy tính bạn ngay từ đầu để ngăn chặn sự xâm nhập.

- Bạn nên tránh nhấp vào các quảng cáo pop-up khi bạn lướt web.

- Không nên mở các file lạ có đính kèm trên email.

- Không nên tải các phần mềm, ứng dụng ở trên các website không đáng tin cậy.

- Bạn nên thường xuyên cập nhật hệ điều hành, ứng dụng.

- Chỉ nên tải các app có lượt tải lớn và thứ hạng cao từ Google Play hay Apple Store,...

- Không nên tải ứng dụng từ các nguồn bên thứ 3.

- Không nên nhấp vào các liên kết lạ, các liên kết không xác định ở trong email hay văn bản và tin nhắn.

Dấu hiệu nhận biết máy tính/website nhiễm Malware

- Các trang pop-up quảng cáo xuất hiện với tần suất dày đặc, tắt không được

- Link dẫn đến một trang web hoàn toàn khác

- Các phần mềm bảo mật liên tục báo lỗi

- Xuất hiện các comment, liên kết spam

b) Tấn công giả mạo (Phishing)

Phishing (Tấn công giả mạo) là hình thức tấn công mạng mà kẻ tấn công giả mạo thành một đơn vị uy tín để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng.

Thông thường, tin tặc sẽ giả mạo thành ngân hàng, trang web giao dịch trực tuyến, ví điện tử, các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin nhạy cảm như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quý giá khác.

Phương thức tấn công này thường được tin tặc thực hiện thông qua email và tin nhắn. Người dùng khi mở email và click vào đường link giả mạo sẽ được yêu cầu đăng nhập. Nếu "mắc câu", tin tặc sẽ có được thông tin ngay tức khắc.

Các phương thức tấn công Phishing

Có nhiều kỹ thuật mà tin tặc sử dụng để thực hiện một vụ tấn công Phishing.

- Giả mạo email

Một trong những kỹ thuật cơ bản trong tấn công Phishing là giả mạo email. Tin tặc sẽ gửi email cho người dùng dưới danh nghĩa một đơn vị/tổ chức uy tín, dụ người dùng click vào đường link dẫn tới một website giả mạo và "mắc bẫy".

Những email giả mạo thường rất giống với email chính chủ, chỉ khác một vài chi tiết nhỏ, khiến cho nhiều người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công.

Để làm cho nội dung email giống thật nhất có thể, kẻ tấn công luôn cố gắng "ngụy trang" bằng nhiều yếu tố:

+ Địa chỉ người gửi

+ Chèn Logo chính thức của tổ chức để tăng độ tin cậy

+ Thiết kế các cửa sổ pop-up giống y hệt bản gốc (cả về màu sắc, font chữ,…)

+ Sử dụng kĩ thuật giả mạo đường dẫn (link) để lừa người dùng

+ Sử dụng hình ảnh thương hiệu của các tổ chức trong email giả mạo để tăng độ tin cậy.

- Giả mạo Website

Thực chất, việc giả mạo website trong tấn công Phishing chỉ là làm giả một landing page chứ không phải toàn bộ website. Trang được làm giả thường là trang đăng nhập để cướp thông tin của nạn nhân. Kỹ thuật làm giả website có một số đặc điểm sau:

+ Thiết kế giống tới 99% so với website gốc

+ Đường link chỉ khác 1 ký tự duy nhất.

+ Luôn có những thông điệp khuyến khích người dùng nhập thông tin cá nhân vào website

- Vượt qua các bộ lọc Phishing

Hiện nay, các nhà cung cấp dịch vụ email như Google hay Microsoft đều có những bộ lọc email spam/phishing để bảo vệ người dùng. Tuy nhiên những bộ lọc này hoạt động dựa trên việc kiểm tra văn bản trong email để phát hiện xem email đó có phải phishing hay không. Hiểu được điều này, những kẻ tấn công đã cải tiến các chiến dịch tấn công Phishing lên một tầm cao mới. Chúng thường sử dụng ảnh hoặc video để truyền tải thông điệp lừa đảo thay vì dùng text như trước đây. Người dùng cần tuyệt đối cảnh giác với những nội dung này.

c) Tấn công từ chối dịch vụ (Dos và DDoS)

DoS là "đánh sập tạm thời" một hệ thống, máy chủ hoặc mạng nội bộ. Để thực hiện được điều này, các Hacker thường tạo ra một lượng Traffic/Request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải. Theo đó, người dùng sẽ không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Một hình thức biến thể của DoS là DDoS:Tin tặc sử dụng một mạng lưới các máy tính (Botnet) để tấn công người dùng.vấn đề ở đây là chính các máy tính thuộc mạng lưới Botnet sẽ không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.

Một số hình thức tấn công DDoS

- Tấn công gây nghẽn mạng

Mục tiêu: Gây quá tải hệ thống mạng bằng lượng truy cập lớn đến từ nhiều nguồn để chặn các truy cập thực của người dùng.

- Tấn công TCP

Mục tiêu: Gây cạn tài nguyên máy chủ, ngăn chặn việc nhận các yêu cầu kết nối mới.

- Tấn công khuếch đại DNS

Mục tiêu: Làm quá tải hệ thống bằng phản hồi từ các bộ giải mã DNS.

Cách phòng chống tấn công DDoS

- Theo dõi lưu lượng truy cập của bạn: Với cách này, bạn có thể phát hiện được các vụ tấn công DDoS nhỏ mà tin tặc vẫn thường dùng để Test năng lực của mạng lưới trước khi tấn công thật sự.

- Nếu bạn có thể xác định được địa chỉ của các máy tính thực hiện tấn công: có thể tạo một danh sách quản lý truy cập trong tường lửa để thực hiện chặn các IP này.

d) Tấn công trung gian

Tấn công trung gian, còn gọi là tấn công nghe lén, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Một khi đã chen vào thành công, chúng có thể đánh cắp dữ liệu trong giao dịch đó.

Các hình thức tấn công trung gian

- Sniffing: là kỹ thuật được sử dụng để nắm bắt các gói dữ liệu vào và ra của hệ thống. Cũng tương tự với việc nghe trộm trong điện thoại. Sniffing được xem là hợp pháp nếu được sử dụng đúng cách. Doanh nghiệp có thể thực hiện để tăng cường bảo mật.

- Packet Injection: Kẻ tấn công sẽ đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp/phần

mềm độc hại bởi chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.

- Gỡ rối phiên: Bạn đã từng gặp thông báo "Phiên hoạt động đã hết hạn" chưa? Nếu đã từng thực hiện thanh toán trực tuyến hoặc điền vào biểu mẫu, hẳn bạn sẽ biết thuật ngữ này. Khoản thời gian từ lúc bạn đăng nhập vào tài khoản ngân hàng của bạn đến khi đăng xuất khỏi tài khoản đó được gọi là một phiên. Các phiên này là mục tiêu của tin tặc. Bởi chúng có khả năng chứa thông tin kín đáo. Trong hầu hết các trường hợp, một Hacker thiết lập sự hiện diện của mình trong phiên. Và cuối cùng nắm quyền kiểm soát nó. Các cuộc tấn công này có thể được thực thi theo nhiều cách khác nhau.

- Loại bỏ SSL: là một loài hiếm khi nói đến các cuộc tấn công trung gian, nhưng cũng là một trong những nguy hiểm nhất. Trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL/TLS và chuyển giao thức từ HTTPS an toàn sang HTTP không an toàn.

Cách phòng chống tấn công trung gian

- Đảm bảo các Website bạn truy cập đã cài SSL.

- Không mua hàng hoặc gửi dữ liệu nhạy cảm khi dùng mạng công cộng.

- Không nhấp vào Link hoặc Email độc hại.

- Có các công cụ bảo mật thích hợp được cài đặt trên hệ thống của bạn.

- Tăng cường bảo mật cho hệ thống mạng của gia đình bạn.

đ) Khai thác lỗ hổng Zero-day

Lỗ hổng zero-day thực chất là những lỗ hổng bảo mật của phần mềm hoặc phần cứng mà người dùng chưa phát hiện ra. Chúng tồn tại trong nhiều môi trường khác nhau như: Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm – phần cứng máy tính, thiết bị IoT, Cloud, …

Sự khác nhau giữa một lỗ hổng bảo mật thông thường và một lỗ hổng Zero-day nằm ở chỗ: Lỗ hổng Zero-day là những lỗ hổng chưa được biết tới bởi đối tượng sở hữu hoặc cung cấp sản phẩm chứa lỗ hổng.

Thông thường ngay sau khi phát hiện ra lỗ hổng 0-day, bên cung cấp sản phẩm sẽ tung ra bản vá bảo mật cho lỗ hổng này để người dùng được bảo mật tốt hơn. Tuy nhiên trên thực tế, người dùng ít khi cập nhật phiên bản mới của phần

mềm ngay lập tức. Điều đó khiến cho Zero-day được biết đến là những lỗ hổng rất nguy hiểm. Có thể gây thiệt hại nghiêm trọng cho doanh nghiệp và người dùng.

Cách phòng chống lỗ hổng Zero-day

- Thường xuyên cập nhật phần mềm và hệ điều hành

- Triển khai giám sát bảo mật theo thời gian thực

- Triển khai hệ thống IDS và IPS

- Sử dụng phần mềm quét lỗ hổng bảo mật

e) Các loại hình tấn công khác

Ngoài ra, còn rất nhiều hình thức tấn công mạng khác như:

- Tấn công chuỗi cung ứng

- Tấn công Email

- Tấn công vào con người

- Tấn công nội bộ tổ chức

Mỗi hình thức tấn công đều có những đặc tính riêng. Và chúng ngày càng tiến hóa phức tạp, tinh vi đòi hỏi các cá nhân, tổ chức phải liên tục cảnh giác & cập nhật các công nghệ phòng chống mới.

4.4. Các giải pháp hạn chế tấn công mạng

Đối với cá nhân

- Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,… Chi tiết tại: 3 kiểu Tấn công Password cơ bản & cách phòng chống

- Hạn chế truy cập vào các điểm Wifi công cộng

- Không sử dụng phần mềm bẻ khóa (crack)

- Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.

- Cẩn trọng khi duyệt Email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.

- Tuyệt đối không tải các File hoặc nhấp vào đường link không rõ nguồn gốc.

- Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.

- Sử dụng một phần mềm diệt Virus uy tín.

Đối với tổ chức, doanh nghiệp

- Xây dựng một chính sách bảo mật với các điều khoản rõ ràng, minh bạch

- Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.

- Tuyệt đối không sử dụng các phần mềm Crack

- Luôn cập nhật phần mềm lên phiên bản mới nhất.

- Sử dụng các dịch vụ lưu trữ đám mây uy tín cho mục đích lưu trữ.

- Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: bảo mật Website, bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng, bảo mật IoT, bảo mật hệ thống CNTT – vận hành…

- Tổ chức các buổi đào tạo, Training kiến thức sử dụng Internet an toàn cho nhân viên.

5. XU HƯỚNG AN TOÀN THÔNG TIN MẠNG

Nguy cơ rủi ro trên không gian mạng sẽ tăng lên đồng thời với việc chuyển đổi sang kỷ nguyên Công nghiệp 4.0. An ninh mạng ngày càng trở nên quan trọng và cũng là vấn đề quan tâm hàng đầu với nhiều tổ chức, doanh nghiệp.

Với việc sử dụng công nghệ ngày càng nhiều trong cuộc sống hàng ngày của chúng ta, tội phạm mạng cũng gia tăng, bằng chứng là các cuộc tấn công mạng đã gây ra 92% tổng số vụ rò rỉ dữ liệu trong quý đầu tiên của năm 2022. Việc cập nhật các xu hướng an ninh mạng là rất quan trọng để chống lại các mối đe dọa, có thể ảnh hưởng đáng kể đến sự phát triển của tổ chức, doanh nghiệp.

Trong những năm tới, an toàn thông tin mạng dự kiến sẽ chứng kiến những xu hướng mới sau đây:

5.1. Bảo mật ứng dụng

Bảo mật ứng dụng bao gồm các biện pháp được thực hiện để cải thiện tính bảo mật của ứng dụng bằng cách tìm, sửa và ngăn chặn các lỗ hổng bảo mật. Các kỹ thuật khác nhau được sử dụng để xác định các lỗ hổng bảo mật như vậy ở các giai đoạn khác nhau của vòng đời ứng dụng, chẳng hạn như thiết kế, phát triển, triển khai, nâng cấp, bảo trì.

Mục tiêu cuối cùng của bảo mật ứng dụng là cải thiện các hoạt động bảo mật và thông qua đó, tìm, sửa chữa và ngăn chặn các nguy cơ gây ảnh hưởng đến sự an toàn của các ứng dụng.

Hệ thống bảo mật ứng dụng làm giảm rủi ro bảo mật liên quan đến các hoạt động khác nhau của các ứng dụng khác nhau, chẳng hạn như web và ứng dụng di động. Các chuyên gia an ninh mạng dự đoán rằng, các ứng dụng web sẽ vẫn là nguyên nhân thường xuyên nhất của các vi phạm đã được xác nhận. Với việc các tổ chức ngày càng kết nối với các ứng dụng quan trọng khác nhau thông qua Internet sẽ làm gia tăng rủi ro cho các ứng dụng.

5.2. Bảo mật đám mây

Sự phổ biến của các ứng dụng và phần mềm đám mây đã tăng lên đáng kể trong những năm gần đây. Trong khi việc sử dụng các dịch vụ đám mây mang lại nhiều lợi ích cho tổ chức, doanh nghiệp và nhân viên, nó cũng đem đến những rủi ro về an ninh mạng mới.

Các ứng dụng và dịch vụ đám mây cho phép người dùng truy cập tệp và dữ liệu từ mọi nơi, điều này khiến chúng dễ dàng trở thành mục tiêu hàng đầu của các tin tặc.

Vì vậy, một trong những điều quan trọng khi sử dụng các dịch vụ đám mây là bất kỳ tài khoản đám mây nào cũng cần được bảo mật đúng cách, sử dụng mật khẩu phức tạp, duy nhất và được trang bị xác thực đa yếu tố, để trong trường hợp mật khẩu bị đánh cắp, rò rỉ vẫn có một rào cản bổ sung giúp ngăn chặn và hạn chế việc tài khoản bị chiếm đoạt và lạm dụng.

5.3. Bảo mật 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 ích và khả năng dễ dàng sử dụng kết nối Internet mọi lúc, mọi nơi. Theo số liệu của Liên minh Viễn thông Quốc tế đưa ra tại thông cáo báo chí "Sự kiện và số liệu 2022" cho thấy, tính đến cuối năm 2022, gần 3/4 dân số toàn cầu từ 10 tuổi trở lên (ước khoảng 73% dân số) sở hữu điện thoại di động.

Tuy nhiên, việc sử dụng nhiều các thiết bị di động cũng làm gia tăng các cuộc tấn công mạng, 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. 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.

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 tổ chức, doanh nghiệp 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.

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.

5.4. Bảo mật cho các thiết bị IoT

Internet vạn vật (IoT) là một mạng lưới rộng lớn bao gồm các thiết bị điện tử, chương trình phần mềm và các danh mục khác có thể kết nối với Internet để chia sẻ dữ liệu. Các thiết bị IoT có trong cuộc sống như: nhiều ô tô hiện đại có thể kết nối với điện thoại di động hoặc đồng hồ thông minh bằng Internet, cho phép chia sẻ hình ảnh, danh sách phát nhạc, dữ liệu vị trí…

Tại nhà, IoT có thể kết nối các thiết bị thông minh như bộ điều nhiệt, tủ lạnh, đèn chiếu sáng và nhiều thiết bị khác, giúp ngôi nhà hoạt động hiệu quả hơn. Trong những môi trường doanh nghiệp, chúng ta có thể thấy các sản phẩm IoT như khóa thông minh, thiết bị giám sát năng lượng và thậm chí cả thiết bị lập lịch thông minh.

IoT đang làm cho cuộc sống của chúng ta trở nên thuận tiện hơn theo nhiều cách. Tuy nhiên, IoT cũng là một công nghệ tương đối mới, có nghĩa là có những

mối đe dọa bảo mật cần lưu ý. Nếu không có các biện pháp bảo vệ tại chỗ, các thiết bị IoT có thể dễ bị tấn công mạng và các mối đe dọa bảo mật khác.

Nhờ việc tự động hóa ngôi nhà bằng cách sử dụng IoT, việc cung cấp thiết bị cho những ngôi nhà thông minh dự kiến sẽ đạt 1,8 tỷ vào năm 2025. Các thiết bị thông minh, nhà thông minh và trợ lý giọng nói đã trở thành một phần không thể thiếu trong cuộc sống của chúng ta. Tuy nhiên, chúng ta cần lưu ý rằng mỗi thiết bị như vậy có thể bị tội phạm mạng tấn công và chiếm đoạt. Dự báo, với việc gia tăng số lượng phương tiện tự lái trên đường trong năm 2024 cũng sẽ làm gia tăng số lượng các cuộc tấn công mạng.

5.5. Bảo mật trong làm việc từ xa

Làm việc từ xa đã trở nên phổ biến và được chấp nhận trên toàn thế giới, đặc biệt khi ngày càng có nhiều tổ chức cho phép phần lớn lực lượng lao động của họ làm việc tại nhà.

Làm việc từ xa đã nới lỏng quyền kiểm soát của các tổ chức, doanh nghiệp đối với việc sử dụng dữ liệu an toàn của nhân viên. Tội phạm mạng, cùng với những kẻ tham gia lừa đảo và tấn công phi kỹ thuật đã lợi dụng kẽ hở này, sử dụng các phương pháp tấn công ngày càng tinh vi để tấn công mạng.

Quản lý xác thực an toàn và quyền truy cập hợp pháp vào dữ liệu của các tổ chức, doanh nghiệp là những phương pháp chính để đảm bảo an toàn cho làm việc từ xa.

Như đã đề cập ở trên, tấn công phi kỹ thuật là một hình thức tấn công đang được các tổ chức, doanh nghiệp chú ý và cũng đang phát triển nhanh chóng. Đây là hình thức tấn công mà đối tượng tấn công tác động trực tiếp đến tâm lý con người (kỹ năng xã hội) để đánh cắp thông tin, dữ liệu của cá nhân, tổ chức. Đối tượng tấn công có thể mạo danh là nhân viên, kỹ thuật viên, công an, hay các nhà nghiên cứu... và đề nghị bạn cung cấp thông tin xác thực để thực hiện một công việc nào đó.

Nhóm tin tặc sẽ đặt câu hỏi để thu thập thông tin từ người dùng, nếu không thể thu thập đủ thông tin từ một nguồn đối tượng tấn công, chúng có thể liên hệ với một nguồn khác cùng tổ chức và dựa vào những thông tin đánh cắp trước đó để tăng thêm độ tin cậy. Trong những năm qua, xu hướng một người dùng bị tấn công bởi các phương thức khác nhau như qua email lừa đảo, tin nhắn SMS và phương tiện truyền thông xã hội đang ngày một gia tăng.

5.6. Bảo hiểm rủi ro trên không gian mạng

Hiện nay, các hình thức lừa đảo qua mạng internet có xu hướng gia tăng mạnh mẽ và ngày càng tinh vi. Các vụ tấn công, lừa đảo trên không gian mạng đã và đang gây ra những thiệt hại không nhỏ cho người sử dụng.

Khách hàng đang sở hữu các tài khoản ngân hàng, ví điện tử… hay các sản phẩm công nghệ như: máy tính cá nhân, điện thoại… có kết nối internet đều có thể trở thành nạn nhân của tội phạm an ninh mạng.

Khi thói quen của người tiêu dùng chuyển từ offline sang online nhiều hơn thì cũng đối mặt với các rủi ro tiềm ẩn trên không gian mạng nhiều hơn. Vì vậy, xu hướng bảo vệ người tiêu dùng khỏi các rủi ro trên không gian mạng đang ngày càng được các tổ chức, cá nhân quan tâm.

Việc bảo hiểm rủi ro trên không gian mạng giúp giảm thiểu các mối đe dọa và tổn thất tài chính từ các cuộc tấn công mạng. Các tổ chức, cá nhân tham gia bảo hiểm sẽ được bồi thường khi bị mất cắp tiền trong tài khoản ngân hàng hoặc ví điện tử, bị đánh cắp dữ liệu, tài khoản kỹ thuật số, bị trộm cắp thông tin cá nhân trên môi trường mạng gây tổn hại về tài chính, uy tín, danh dự.

5.7. Bảo mật Zero Trust

Mô hình bảo mật Zero Trust có nghĩa là không nên tin bất kỳ thứ gì bên trong và ngoài hệ thống mạng đang được sử dụng và chỉ nên áp dụng các biện pháp bảo mật tại nơi nào cần đến, phân chia thành ngăn và bảo vệ những hệ thống, dữ liệu quan trọng. Nói cách khác, mục đích của Zero Trust là bảo đảm ngay cả khi một tài sản bị xâm phạm, điều này cũng không làm tổn hại đến cả tổ chức, doanh nghiệp.

Mặc dù cách tiếp cận Zero Trust sẽ không ngăn chặn tội phạm mạng đánh cắp thông tin. Tuy nhiên, Zero Trust sẽ làm chậm quá trình đánh cắp thông tin và khiến những tên tội phạm mạng phải cố gắng nhiều hơn để truy cập dữ liệu, đặc biệt là các loại dữ liệu nhạy cảm nhất, thường sẽ yêu cầu mức độ xác thực cao không chỉ dựa vào tên người dùng và mật khẩu.

Việc áp dụng các giải pháp bảo mật Zero Trust sẽ được mở rộng trên nhiều tổ chức tư nhân và chính phủ hơn nữa để chống lại bối cảnh mối đe dọa ngày càng tăng. Với nhiều tổ chức thống nhất cách tiếp cận của họ để giải quyết các rủi ro an ninh mạng, việc áp dụng chiến lược Zero Trust có thể mang lại khả năng cải thiện tình hình bảo mật tổng thể của tổ chức, doanh nghiệp.

5.8. Trí tuệ nhân tạo

Trí tuệ nhân tạo (AI) là một thuật ngữ rộng bao gồm nhiều loại công nghệ, từ các thuật toán đơn giản đến các hệ thống phức tạp hơn. Nói một cách đơn giản, AI là một hệ thống máy tính có thể thực hiện các nhiệm vụ thường đòi hỏi trí thông minh của con người, chẳng hạn như hiểu ngôn ngữ tự nhiên và nhận dạng các đối tượng.

Tuy nhiên, AI không ngừng phát triển và ngày càng trở nên tinh vi hơn. Thế hệ AI mới nhất có khả năng thực hiện nhiều hơn những tác vụ đơn giản. Những hệ thống này có thể học hỏi và cải thiện theo thời gian, khiến chúng trở nên mạnh mẽ hơn.

AI đã được sử dụng thành công trong việc tăng cường bảo mật và cải thiện an ninh mạng cho các tổ chức, doanh nghiệp như sử dụng AI giúp phát hiện, quản lý lỗ hổng bảo mật và phản ứng với các mối đe doạ nhanh hơn nhiều so với khả năng của con người.

Bên cạnh đó, các tổ chức, doanh nghiệp cũng có thể sử dụng AI để tự động hóa các tác vụ. Điều này có thể giải phóng thời gian cho các chuyên gia bảo mật để họ có thể tập trung vào các nhiệm vụ quan trọng hơn. Nó cũng có thể giúp giảm thiểu khả năng xảy ra lỗi của con người, đây là một trong những nguyên nhân hàng đầu gây ra vi phạm dữ liệu.

5.9. Công cụ phát hiện tấn công mạng

Mỗi cuộc tấn công mạng đều có khả năng dẫn đến hậu quả nghiêm trọng vì các biện pháp bảo vệ không được áp dụng hoặc hiện không khả dụng. Việc rò rỉ dữ liệu có thể tiêu tốn hàng triệu USD và số tiền này phụ thuộc trực tiếp vào loại tấn công và thời gian của nó, cũng như tổn thất về danh tiếng, lòng trung thành của khách hàng và chính khách hàng. Bất kỳ tổ chức, doanh nghiệp nào lưu trữ dữ liệu trên mạng đều có thể bị tấn công.

Cách duy nhất để các tổ chức, doanh nghiệp có thể ngăn chặn một cuộc tấn công hoặc giảm tác động của nó là xác định hoạt động bất thường trên toàn bộ hệ sinh thái người dùng, ứng dụng và cơ sở hạ tầng của họ. Đó là lý do tại sao các nhà cung cấp các giải pháp bảo mật sẽ ngày càng sử dụng nhiều hơn các công nghệ như AI và học máy để giúp phát hiện sớm các cuộc tấn công mạng.

5.10. Thuê ngoài các dịch vụ an ninh mạng

Khi các cuộc tấn công mạng ngày càng trở nên tinh vi, nhiều tổ chức, doanh nghiệp cần sự trợ giúp của các nhà cung cấp giải pháp bảo mật chuyên nghiệp để đảm bảo mức độ bảo mật cao. Do đó, xu hướng bảo vệ tổ chức, doanh nghiệp bằng các nhà cung cấp dịch vụ bảo mật chuyên nghiệp sẽ nở rộ trong năm 2023, 2024 cũng như những năm tới.

Những nhà cung ứng dịch vụ bảo mật chuyên nghiệp đều là những doanh nghiệp hàng đầu, có kinh nghiệm, kiến thức chuyên môn và công nghệ phong phú giúp theo dõi các mối đe dọa bảo mật, cập nhật hệ thống và giảm thiểu các lỗ hổng với chi phí phải chăng.

Họ cung cấp các lớp bảo mật phù hợp, bao gồm bản vá phần mềm, bảo mật hệ thống tên miền (DNS), tường lửa, phần mềm chống phần mềm độc hại, chống lừa đảo, trình quản lý thông tin xác thực,… để bảo vệ thông tin bí mật cho khách hàng. Các nhà cung cấp này cũng sẽ thực hiện giám sát tài sản và mạng 24/7 bằng cách sử dụng nhiều công cụ chuyên dụng như AI để xác định các điểm bất thường và tránh sự gián đoạn ngoài ý muốn.

5.11. Sự gia tăng của các cuộc tấn công phá hủy

Với bối cảnh chính trị hiện tại, các chuyên gia bảo mật của Kaspersky dự đoán rằng sẽ có một số lượng lớn các cuộc tấn công mạng gây rối và phá hủy xảy ra vào năm tới, ảnh hưởng đến cả khu vực chính phủ và các ngành công nghiệp mũi nhọn. Có khả năng rằng một phần trong số chúng sẽ không dễ dàng truy vết được từ các sự cố mạng và sẽ trông như các sự cố ngẫu nhiên. Phần còn lại sẽ ở dạng tấn công giả dạng mã độc tống tiền hoặc các hoạt động xâm nhập bất hợp pháp. Ngoài ra, các chuyên gia bảo mật cũng lo ngại rằng tần suất các cuộc tấn công mạng quy mô lớn có thể diễn ra nhiều hơn nhằm vào cơ sở hạ tầng dân sự, chẳng hạn như mạng lưới điện năng lượng hoặc phát sóng công cộng cũng có thể trở thành mục tiêu, cũng như sự an toàn của cáp quang biển - vốn rất khó bảo vệ trước các tác động vật lý.

5.12. Máy chủ mail trở thành mục tiêu hàng đầu

Trong thời gian vừa qua, hai gã khổng lồ dịch vụ mail là Microsoft Exchange và Zimbra đều phải đối mặt với các lỗ hổng nghiêm trọng. Kaspersky dự báo rằng trong năm 2023 máy chủ mail sẽ trở thành các mục tiêu hàng đầu của tin tặc, bởi các máy chủ này chứa các thông tin tình báo quan trọng mà các tin tặc APT quan tâm và sở hữu bề mặt tấn công lớn để chúng khai thác.

Năm 2023, 2024 rất có thể sẽ chứng kiến nhiều hơn những lỗ hổng "zero-day" đối với các nền tảng, chương trình email khác nhau. Vì vậy, các chuyên gia khuyến nghị quản trị viên hệ thống của các tổ chức, doanh nghiệp cần triển khai các giải pháp giám sát và phát hiện xâm nhập để chủ động ứng phó trước những mối đe dọa này.

5.13. Mã độc Wannacry thế hệ tiếp theo

Theo thống kê, những cuộc tấn công mạng lớn nhất và gây ảnh hưởng nhiều nhất sẽ xảy ra sau khoảng từ 6 đến 7 năm. Trong đó có thể nhắc đến cuộc tấn công do WannaCry tiến hành, sử dụng lỗ hổng để tự động phát tán mã độc tống tiền đến máy tính.

Các chuyên gia bảo mật Kaspersky tin rằng khả năng cao một WannaCry thế hệ tiếp theo sẽ xuất hiện trong năm 2023, 2024. Lý do có thể giải thích cho sự việc này là các tin tặc chuyên nghiệp trên thế giới có khả năng sở hữu ít nhất một phương thức khai thác phù hợp, cùng với sự căng thẳng trên toàn cầu hiện tại làm gia tăng khả năng tấn công và rò rỉ dữ liệu có thể xảy ra.

5.14. Hướng mục tiêu đến các công nghệ, nhà sản xuất vệ tinh

Kaspersky từng phát hiện một nhóm tin tặc chiếm quyền điều khiển thông tin liên lạc vệ tinh, đồng thời cũng đã có những bằng chứng cho thấy các nhóm APT có khả năng tấn công vệ tinh. Có khả năng tin tặc sẽ ngày càng chú ý đến việc thao túng và can thiệp vào các công nghệ vệ tinh trong tương lai, khiến cho việc bảo mật các công nghệ này trở nên quan trọng hơn bao giờ hết./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG