AN TOÀN THÔNG TIN MẠNG CHO NGƯỜI TIÊU DÙNG TRÊN KHÔNG GIAN MẠNG TRONG TÌNH HÌNH MỚI

VŨ NGỌC HƯNG
Cục An toàn thông tin - Bộ Thông tin và Truyền thông

Trong thời gian qua, đại dịch COVID-19 đã ảnh hưởng đến hầu như tất cả các khía cạnh của cuộc sống của chúng ta. Cách ly xã hội, dừng phương tiện công cộng, hạn chế đi lại, v.v.. và nhiều hơn nữa. Chúng ta thấy xu hướng trong việc chuyển đổi sang sử dụng không gian mạng xuất hiện từ tác động của COVID-19 đó là: mọi người chuyển sang các nền tảng kỹ thuật số cho nhu cầu hàng ngày như khám chữa bệnh từ xa, mua sắm trực tuyến, thanh toán trực tuyến, làm việc từ xa...

Trong hơn 02 năm diễn ra đại dịch, chứng kiến sự bùng nổ của các cuộc tấn công mạng vào các doanh nghiệp, cơ sở hạ tầng quan trọng, cơ sở chăm sóc sức khỏe, cơ quan chính phủ, trường học và hơn thế nữa. Những cuộc tấn công này đã được các phương tiện truyền thông đưa tin ở mức độ dày đặc. Có thể kể đến các cuộc tấn công điển hình vào Kia Motors America, Colonial Pipeline, JBS - nhà cung cấp thịt bò lớn nhất thế giới, Twitter, Zoom,... đã lấy cắp hàng triệu thông tin khách hàng hay làm sập hệ thống, gián đoạn sản xuất, đồng thời làm thiệt hại kinh tế vô cùng lớn.

Các cuộc tấn công này sẽ không dừng lại, dự báo tội phạm mạng sẽ gây thiệt hại cho thế giới đến 10,5 nghìn tỷ USD mỗi năm vào năm 2025. Tuy nhiên, những con số này chủ yếu được quy cho các doanh nghiệp - không có nhiều sự chú trọng vào người tiêu dùng cá nhân. Vì các phương tiện truyền thông chủ yếu đưa tin về những câu chuyện tấn công doanh nghiệp gây nên các con số thiệt hại khổng lồ, hiếm khi truyền thông đưa tin về các vụ tấn công mạng vào cá nhân và mức độ thiệt hại. Nhưng trong tương lai, điều này cần phải thay đổi.

Trong quá trình chuyển đổi số, người tiêu dùng sẽ bị ảnh hưởng nhiều hơn bao giờ hết bởi các mối đe dọa trên không gian mạng. Theo đó, chúng ta cần đảm bảo rằng an ninh mạng không bỏ mặc người tiêu dùng.

Các mối đe dọa an ninh mạng chống lại người tiêu dùng

Công nghệ đã trở nên quan trọng hơn trong cả cuộc sống làm việc và cá nhân của chúng ta. Bất chấp sự gia tăng của nhu cầu công nghệ, có thể nhận thấy rằng nhiều tổ chức vẫn chưa cung cấp một môi trường làm việc từ xa đảm bảo "an toàn trên mạng". Nơi mà các cuộc họp kinh doanh trước đây thường được tổ chức trực tiếp, hầu hết giờ đây diễn ra ảo.

Đại dịch đã kéo dài mạng lưới của các doanh nghiệp, đẩy nhanh quá trình chuyển đổi kỹ thuật số và khiến hoạt động của các doanh nghiệp có khả năng tiếp xúc với nhiều tội phạm mạng hơn. Do vậy, an toàn thông tin mạng (hay an ninh mạng) ngày càng quan trọng trong hoạt động của các tổ chức, cá nhân.

Sự gia tăng các hoạt động làm việc từ xa kêu gọi sự tập trung nhiều hơn vào an ninh mạng, vì nguy cơ an ninh mạng ngày càng lớn. Điều này ngày càng rõ ràng, chẳng hạn, từ thực tế là rất nhiều người tiêu dùng rơi vào tình trạng bị lừa đảo trực tuyến khi đang làm việc, giải trí, mua sắm trực tuyến,... tại nhà. Những kẻ tấn công mạng coi đại dịch là cơ hội để đẩy mạnh các hoạt động tội phạm của chúng bằng cách khai thác lỗ hổng của các cá nhân hoạt động trên không gian mạng tại nhà và lợi dụng sự quan tâm mạnh mẽ của mọi người đối với tin tức liên quan đến coronavirus (ví dụ như các trang web liên quan đến coronavirus giả mạo độc hại).

Tội phạm khai thác các điểm yếu an ninh mạng trong làm việc từ xa là hàng loạt cuộc tấn công mạng vào các dịch vụ hội nghị truyền hình. Từ tháng 2 năm 2020 đến tháng 5 năm 2020, hơn nửa triệu người đã bị ảnh hưởng bởi các vi phạm trong đó dữ liệu cá nhân của người dùng dịch vụ hội nghị truyền hình (tên, mật khẩu, địa chỉ email) đã bị đánh cắp và bán trên dark web. Tin tặc cũng tấn công hệ thống mạng của các công ty để truy cập thông tin đăng nhập của nhân viên và dữ liệu bị đánh cắp sau đó được bán cho các tội phạm an ninh mạng khác. Một trong những hậu quả là sự gián đoạn nghiêm trọng đối với các doanh nghiệp phụ thuộc nhiều vào nền tảng hội nghị truyền hình. Theo đó tin tặc sử dụng các tổ hợp tên người dùng và mật khẩu đã đánh cắp trước đó để truy cập vào các tài khoản khác. Điều này là có thể xảy ra vì rất phổ biến các cá nhân sử dụng cùng một tổ hợp tên người dùng/mật khẩu trên nhiều tài khoản.

Nhiều trường hợp đã ghi nhận các thành viên không mong muốn và không được mời có quyền truy cập vào các cuộc họp ảo và lấy thông tin bí mật hoặc nhạy cảm, sau đó được bán cho một bên khác hoặc cung cấp cho công chúng để làm tổn hại danh tiếng của công ty.

Hầu hết các mối đe dọa này đã tăng cường do các cơ hội xuất hiện trong đợt bùng phát COVID-19.

Một trong những lý do khiến các cuộc tấn công mạng tăng đột biến có thể là do một số doanh nghiệp vừa và nhỏ áp dụng chính sách nhân viên có thể sử dụng thiết bị cá nhân của họ (điện thoại, máy tính bảng hoặc máy tính xách tay) để truy cập thông tin của công ty. Làm việc tại nhà không đảm bảo mức độ an ninh mạng như môi trường văn phòng. Khi sử dụng máy tính cá nhân hoặc máy tính xách tay để truy cập các tệp và dữ liệu của công ty (ngay cả với sự bảo mật của giải pháp MDM - quản lý thiết bị di động), người dùng dễ bị tấn công mạng hơn. Ví dụ: nhân viên có thể

không thường xuyên quét chống vi-rút hoặc chống phần mềm độc hại. Môi trường làm việc tại nhà thường không có các biện pháp phòng chống tấn công mạng như hệ thống tại trụ sở các doanh nghiệp. Ngoài ra, mạng Wi-Fi gia đình dễ bị tấn công hơn nhiều.

Lỗi của con người là một vấn đề đáng quan tâm khác. Trước đại dịch, lỗi của con người đã là nguyên nhân chính gây ra "mất an ninh mạng" tại cơ quan, doanh nghiệp (vô tình hoặc tin tưởng nhầm người nên cung cấp quyền truy cập cho tin tặc).

Tuy nhiên, khi đại dịch xảy ra, với chế độ làm việc tại nhà, vấn đề còn lớn hơn. Khi họ làm việc tại nhà, nhân viên có thể bị các thành viên trong gia đình hoặc nhiều người khác làm gián đoạn công việc họ đang làm. Những phiền nhiễu này có thể làm cho các cá nhân trở nên bất cẩn hơn. Hệ thống CNTT cần phải thích ứng với những thay đổi này trong thực tiễn làm việc và sự gia tăng lỗi của con người. Điều này có thể được thực hiện bằng nhiều cách, chẳng hạn như kết hợp thời gian chờ trong các hệ thống thông tin quan trọng, tăng cường kiểm soát, thực thi phân tách nhiệm vụ hoặc kiểm soát tự động.

Nhiều tội phạm mạng đang tận dụng những gì chúng học được từ việc tấn công các doanh nghiệp và bắt đầu sử dụng những kỹ năng đó để tấn công người tiêu dùng. Rất nhiều tài liệu hướng dẫn trên Internet được sử dụng để truyền những kỹ năng này và hầu hết người tiêu dùng hoàn toàn không biết rằng họ có khả năng trở thành mục tiêu. Các nhà nghiên cứu gần đây đã phát hiện một công cụ khai thác mật mã được gắn vào một bản tải xuống torrent của phim Người Nhện.

Các tổ chức quy mô lớn có thể sẵn sàng và có khả năng chuẩn bị để phòng, chống các cuộc tấn công mạng của tội phạm mạng, nhưng nhiều người tiêu dùng thì không. Các doanh nghiệp thường thực hiện vá các lỗ hổng bảo mật trong hệ thống công nghệ thông tin của mình khi chúng xuất hiện, nhưng người tiêu dùng thường không biết về các lỗ hổng này, thậm chí không quan tâm. Và trong khi nhiều doanh nghiệp có đội ngũ nhân viên công nghệ thông tin có thể tận dụng công nghệ mới máy học như một phương pháp phát hiện và phản hồi để loại bỏ các mối đe dọa về an ninh mạng chưa từng biết trước đây, thì người tiêu dùng cá nhân không phải lúc nào cũng có trong tầm tay sức mạnh này.

MỘT SỐ VỤ TẤN CÔNG MẠNG ĐIỂN HÌNH

Kia Motors America được cho là đã trở thành nạn nhân của một cuộc tấn công bằng ransomware đòi số bitcoin trị giá hơn 20 triệu đô la vào tháng 02/2021.

Colonial Pipeline: vụ tấn công đã đánh sập đường ống dẫn nhiên liệu lớn nhất ở Hoa Kỳ và dẫn đến tình trạng thiếu hụt nhiên liệu trên khắp Bờ Đông vào tháng 6/2021.

JBS - nhà cung cấp thịt bò lớn nhất thế giới, đã trả cho các tin tặc ransomware xâm phạm mạng máy tính của họ khoảng 11 triệu đô la. Công ty đã bị tấn công vào tháng 5/2021, dẫn đến việc các nhà máy sản xuất thịt trên khắp Hoa Kỳ và Úc phải đóng cửa trong ít nhất một ngày.

Twitter đã bị tấn công thông qua một chiến dịch lừa đảo qua điện thoại, mục tiêu là các tài khoản của hơn 130 nhân vật nổi tiếng.

Tội phạm mạng cũng đã đánh cắp hơn 500.000 mật khẩu Zoom và đưa thông tin đăng nhập rao bán trên dark web; tấn công MGM Resorts và Marriott International và làm lộ dữ liệu của hàng triệu khách hàng.

Magellan Health đã trải qua một cuộc tấn công bằng ransomware và vi phạm dữ liệu ảnh hưởng đến 365.000 bệnh nhân.

Hơn nữa, bây giờ việc làm việc tại nhà đã trở nên phổ biến, nhiều cá nhân đang thấy mình nằm ngoài sự an toàn của mạng lưới an ninh mạng của công ty. Những kẻ tấn công sẽ khai thác điều này bằng cách xâm nhập vào hệ thống gia đình của cá nhân và từ đó, truy cập vào mạng công ty rộng lớn hơn.

Sự phát triển liên tục của Ransomware. Các khoản thanh toán tiền chuộc cho ransomware trong nửa đầu năm 2021 là 570,000 đô la, tăng 82% so với nửa đầu năm 2020. Con số đó sẽ tiếp tục tăng khi các cuộc tấn công ransomware ngày càng tinh vi và mục tiêu là người tiêu dùng ngày càng được quan tâm. Trong tương lai, các tập đoàn, chính phủ sẽ hạn chế việc trả tiền chuộc cho các cuộc tấn công ransomware để chúng trở nên kém hấp dẫn hơn.Tuy nhiên, đối với người dùng cuối, tội phạm mạng không cần phải thực hiện quá trình tấn công ransomware quá phức tạp - và điều này đã dẫn đến nhiều cuộc tấn công hơn. Sự phổ biến của tiền điện tử cũng là một yếu tố chính trong sự phát triển của ransomware do yếu tố ẩn danh. Những cuộc tấn công này sẽ tiếp tục diễn ra vào năm 2022 trừ khi chúng ta phải nỗ lực hơn trong các giải pháp ngăn chặn chúng.

Thông qua các ứng dụng trò chơi giải trí. Vào tháng 3/2021, các nhà nghiên cứu từ Cisco Talos xác định phần mềm độc hại được nhúng bên trong phần mềm gian lận cho nhiều trò chơi mà khi người tiêu dùng tải xuống, đã lây nhiễm toàn bộ hệ điều hành của họ. Vào tháng 6/2021, họ đã phát hiện tội phạm mạng đã kiếm được hơn 2 triệu đô la từ một kế hoạch theo đó chúng giấu một phần mềm khai thác tiền điện tử bên trong một trò chơi đã bẻ khóa được hàng nghìn người tải xuống.

Những loại mối đe dọa này sẽ tiếp tục tồn tại và phát triển trong tương lai và trở nên phổ biến hơn khi số lượng game thủ trên toàn thế giới tiếp tục tăng lên. Những người chơi game có thể trở thành mục tiêu dễ dàng cho những kẻ lừa đảo do phần lớn là nhóm tuổi mà trò chơi hiện nay thu hút. Người tiêu dùng này thường ngây thơ và họ có thể dễ dàng bị ép buộc cung cấp thông tin cá nhân.

Giải pháp nào để tăng cường an toàn thông tin mạng cho người tiêu dùng?

Tác động lớn khác của các cuộc tấn công mạng của doanh nghiệp đối với người tiêu dùng là khi một cuộc tấn công vi phạm dữ liệu khách hàng. Nhiều loại tấn công

khiến khách hàng dễ bị đánh cắp danh tính và các loại gian lận khác. Khi những kẻ tấn công bán dữ liệu khách hàng trên dark web và những tên tội phạm khác mua dữ liệu đó, chúng có thể biến một cuộc tấn công doanh nghiệp thành hàng trăm cuộc tấn công người tiêu dùng khác. Nó có thể biến thành gian lận thẻ tín dụng, đánh cắp danh tính,... Các cuộc tấn công mạng có thể xảy ra một lần, nhưng gian lận liên quan đến danh tính và dữ liệu người tiêu dùng là mãi mãi.

Do vậy, người tiêu dùng cần phải được đảm bảo an toàn trong mọi hoạt động trên không gian mạng, các công ty cần phải có biện pháp sẵn sàng phòng, chống những vụ tấn công mạng bằng mọi giá. Dưới đây là một số phương pháp để tăng cường an toàn, an ninh thông tin cho người tiêu dùng trên không gian mạng.

1. Đối với người tiêu dùng, khi sử dụng không gian mạng để làm việc, mua sắm, thanh toán trực tuyến,... tại nhà thông qua máy tính cá nhân (và thậm chí cả những người sử dụng thiết bị thuộc sở hữu của công ty) nên thực hiện các giải pháp:

- Bảo vệ chống vi-rút: Sử dụng phần mềm chống vi-rút và chống phần mềm độc hại trên máy tính. Mặc dù điều này không cung cấp khả năng bảo vệ an toàn dự phòng, nhưng nó loại bỏ nhiều cuộc tấn công cấp thấp.

- Nhận thức về an ninh mạng: Người tiêu dùng nên tìm hiểu về các phương pháp và quy trình tốt nhất để thực hiện việc truy cập Internet như gửi, nhận email sử dụng dịch vụ lưu trữ trên đám mây,...

- Nhận thức về lừa đảo trực tuyến: Người tiêu dùng nên cảnh giác khi nhận được các thông tin, yêu cầu từ Internet và nên kiểm tra tính xác thực của thông tin, địa chỉ người gửi.

- Bảo mật mạng gia đình: Đảm bảo rằng Wi-Fi tại nhà của mình được bảo vệ bằng mật khẩu mạnh.

- Sử dụng VPN: Mạng riêng ảo bổ sung thêm một lớp bảo vệ cho việc sử dụng Internet tại nhà, có thể là một rào cản hữu ích chống lại các cuộc tấn công mạng.

2. Đối với các tổ chức, doanh nghiệp, có một số chiến lược an ninh mạng cơ bản có thể áp dụng.

- Luôn cập nhật các phương pháp mã hóa. Công nghệ mã hóa đang phát triển với tốc độ rất nhanh. Bằng cách luôn cập nhật chúng, các công ty đảm bảo an ninh tối ưu cho khách hàng của họ. Mã hóa dữ liệu cung cấp khả năng bảo vệ và bảo mật dữ liệu hoàn chỉnh trên nhiều thiết bị. Các công ty nên sử dụng mã hóa để bảo vệ dữ liệu được lưu trữ và gửi khỏi tin tặc.

- Hạn chế quyền truy cập thông tin người tiêu dùng. Hạn chế quyền truy cập thông tin người tiêu dùng là một cách hiệu quả khác để bảo vệ dữ liệu người tiêu dùng. Các công ty cần thực hiện các thực hành ủy quyền và xác thực để tăng cường bảo mật. Với các giao thức ủy quyền tại chỗ, các tổ chức có thể giới hạn và hạn chế quyền truy cập thông tin của người dùng. Điều này đảm bảo rằng người dùng chỉ có quyền truy cập vào thông tin liên quan đến họ, do đó bảo vệ các tài nguyên và dữ liệu nhạy cảm.

Quy trình xác thực cũng rất cần thiết vì chúng xác minh người yêu cầu quyền truy cập. Xác thực đa yếu tố (MFA) là một trong những phương pháp xác thực khá an toàn. Nó tăng cường bảo mật tài khoản bằng cách yêu cầu nhiều hình thức xác minh để có được quyền truy cập.

- Xác định quyền riêng tư của người tiêu dùng là ưu tiên hàng đầu. Trong thời đại kỹ thuật số, các tổ chức trên tất cả các ngành đều lưu trữ một lượng lớn dữ liệu. Các tổ chức cần quản lý và kiểm soát khả năng sử dụng, khả năng truy cập, tính toàn vẹn và bảo mật của dữ liệu của họ theo các chính sách dữ liệu nội bộ thích hợp. Ví dụ: ở Liên minh châu Âu, các công ty cần tuân thủ Quy định chung về bảo vệ dữ liệu (GDPR), quy định này đặt ra tiêu chuẩn cho việc truyền dữ liệu. Đạo luật Quyền riêng tư của Người tiêu dùng California (CCPA) là một đạo luật tương tự của tiểu bang nhằm tăng cường bảo vệ người tiêu dùng. Theo các quy định này, các công ty phải tiết lộ bất kỳ việc thu thập dữ liệu nào, mục đích thu thập dữ liệu, họ sẽ lưu giữ dữ liệu trong bao lâu và liệu họ có chia sẻ dữ liệu đó với bất kỳ bên thứ ba nào hay không.

Người tiêu dùng cũng cần được truy cập tất cả thông tin mà các công ty có về họ và cách họ sử dụng thông tin đó. Điều này không chỉ giúp bảo vệ dữ liệu hợp pháp cho các cá nhân mà còn tạo ra sự minh bạch, giúp xây dựng lòng tin giữa công ty và người tiêu dùng.

- Luôn cập nhật những xu hướng công nghệ mới nhất. Công nghệ không ngừng phát triển, và các doanh nghiệp cần phải bắt kịp với nó. Các tổ chức cần duy trì hệ thống công nghệ của mình và luôn cập nhật các xu hướng bảo mật mới nhất có thể.

Việc thay đổi nhận thức về vị trí của người tiêu dùng trên không gian mạng là hết sức cần thiết trong giai đoạn này. Cung cấp nhiều kiến thức hơn, hiểu biết nhiều hơn, nhiều giải pháp sẵn sàng phòng, chống tấn công mạng và các quy định quản lý thích hợp sẽ hạn chế tối đa ảnh hưởng của các mối đe dọa trên không gian mạng đến người tiêu dùng. ■ THÔNG TIN & TRUYỀN THÔNG