Tìm hiểu về bảo mật thiết bị đầu cuối (endpoint security)

Endpoint là gì?

Hệ thống công nghệ thông tin của chúng ta ngày càng phát triển, Internet có tốc độ đường truyền ngày càng cao, các thiết bị công nghệ thông tin cũng ngày càng đa dạng hơn, nhưng mọi sự phát đều có hai mặt. Thế giới công nghệ thông tin hiện đại mang lại nhiều lợi ích nhưng cũng là điều kiện thuận lợi cho những kẻ xấu tận dụng và thực hiện những hành vi phi pháp. Trong đó giải pháp an ninh điểm cuối (endpoint) tức là tích hợp biện pháp bảo vệ an ninh vào các thiết bị tin học ở mọi điểm phân tán cuối cùg có thể là một giải pháp phòng ngừa hiệu quả. Các thiết bị điểm cuối phổ biến nhất bao gồm PC (máy chủ, máy bàn, máy tính xách tay), thiết bị di động, thiết bị lưu trữ kể cả qua USB, các thiết bị Bluetooth, máy đọc mã sản phẩm, máy bán hàng….

Endpoint security là gì?

Endpoint security hoặc Endpoint protection, tạm dịch là bảo mật thiết bị đầu cuối hay bảo mật điểm cuối, là một thuật ngữ đề cập đến một công nghệ bảo vệ mạng máy tính được kết nối từ xa tới các thiết bị của người dùng. Việc sử dụng máy tính xách tay, máy tính bảng, điện thoại di động và các thiết bị không dây khác được kết nối với mạng doanh nghiệp, tạo ra những lỗ hổng bảo mật dễ bị tổn thương và kéo theo các mối đe dọa an ninh. Bảo mật thiết bị đầu cuối là cố gắng đảm bảo

rằng các thiết bị như vậy được an toàn theo một mức độ nhất định theo các yêu cầu và tiêu chuẩn. Nó bao gồm trạng thái giám sát, phần mềm và các hoạt động. Phần mềm bảo vệ điểm cuối sẽ được cài đặt trên tất cả các máy chủ mạng và trên tất cả các thiết bị đầu cuối.

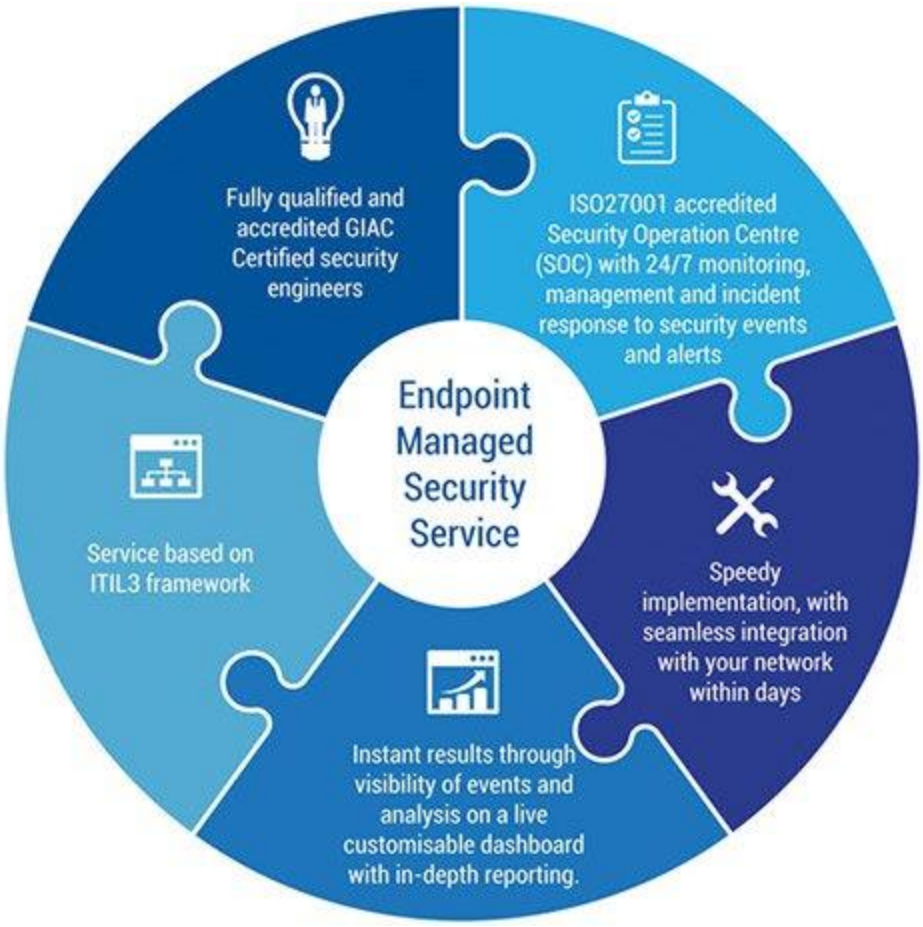
Tương ứng với sự gia tăng của các thiết bị di động như máy tính xách tay, điện thoại thông minh, máy tính bảng… chính là sự gia tăng mạnh về số lượng thiết bị mất hoặc bị đánh cắp. Những sự cố này có khả năng khiến các tổ chức, cá nhân làm thất lạc các dữ liệu nhạy cảm, đặc biệt là đối với các doanh nghiệp cho phép nhân viên của họ mang các thiết bị di động kể trên vào hệ thống mạng doanh nghiệp của họ.

Để giải quyết vấn đề này, các doanh nghiệp phải cung cấp các biện pháp bảo mật dữ liệu doanh nghiệp ngay trên các thiết bị di động của nhân viên của họ theo cái cách mà ngay cả khi thiết bị đó rơi vào tay kẻ xấu, dữ liệu vẫn sẽ được bảo vệ. Quá trình bảo mật thiết bị đầu cuối cho doanh nghiệp này được gọi là bảo mật thiết bị đầu cuối.

Hệ thống quản lý an ninh thiết bị đầu cuối là một cách tiếp cận phần mềm giúp xác định và quản lý máy tính của người sử dụng để truy cập trong mạng của công ty. Điều này liên quan đến việc quản trị mạng để hạn chế truy cập một số trang web nhất định cho người sử dụng để duy trì và tuân thủ các chính sách và tiêu chuẩn của tổ chức. Các thành phần tham gia vào việc sắp xếp các hệ thống quản lý an ninh thiết bị đầu cuối bao gồm một máy tính VPN, một hệ điều hành và một phần mềm chống virus hiện đại. Các thiết bị máy tính mà không phù hợp với chính sách của tổ chức chỉ được cung cấp truy cập có giới hạn vào một mạng LAN ảo. Nó cũng giúp các doanh nghiệp ngăn chặn thành công bất kỳ việc lạm dụng dữ liệu nào của các nhân viên mà họ đã cung cấp dữ liệu. Ví dụ: Một nhân viên bất mãn cố gắng gây phiền toái cho doanh nghiệp hoặc một người có thể là bạn của nhân viên đang cố sử dụng trái phép dữ liệu doanh nghiệp có sẵn trên thiết bị.

Endpoint security thường bị nhầm lẫn với một số công cụ bảo mật mạng khác như chống virus, tường lửa và thậm chí là cả bảo mật mạng.

Tại sao lại được gọi là endpoint security?



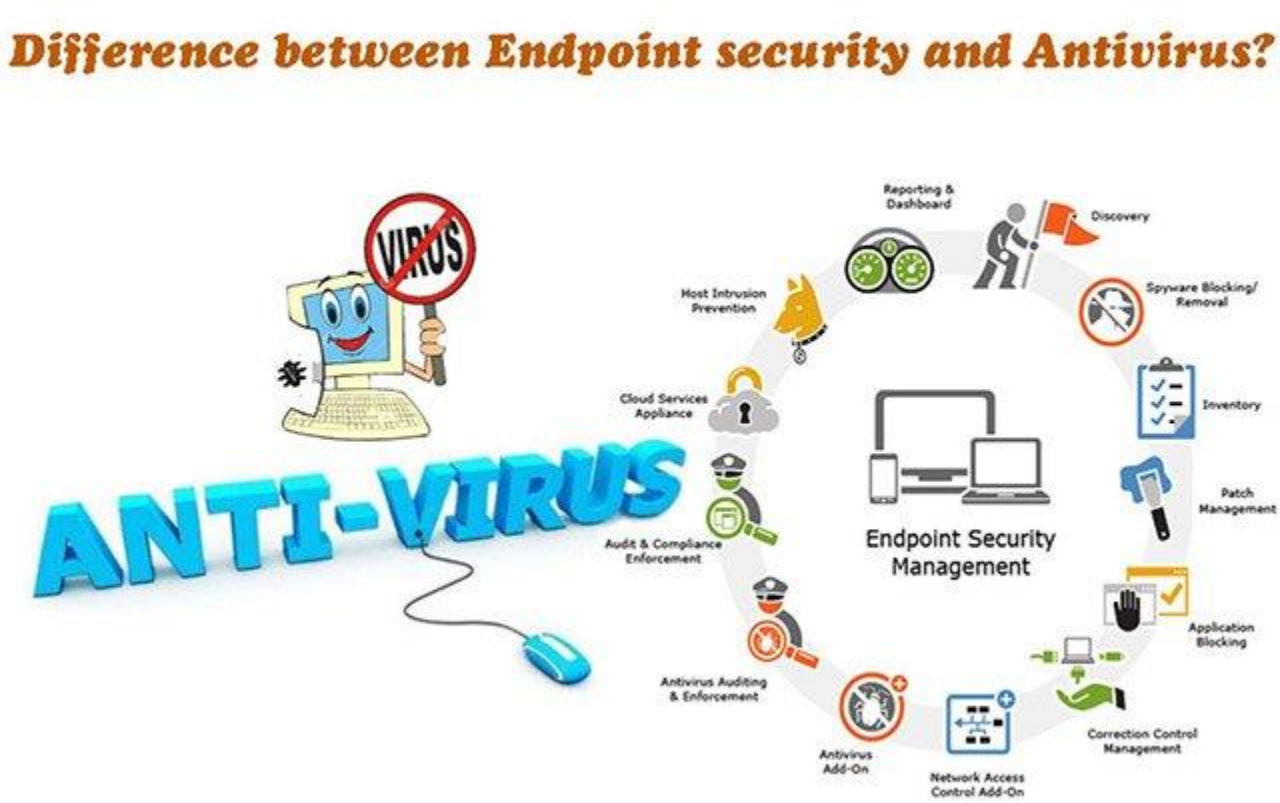
Như bạn có thể thấy, mọi thiết bị có thể kết nối với mạng đều có thể gây ra những nguy cơ bảo mật đáng kể. Và vì các thiết bị này được đặt bên ngoài hệ thống tường lửa của công ty, chúng được gọi là các điểm cuối. Có nghĩa là điểm cuối của hệ thống mạng đó.

Như đã nêu ở mục đầu, điểm cuối có thể là bất kỳ thiết bị di động nào, từ máy tính xách tay đến máy tính bảng ngày nay, miễn là chúng đều có thể được kết nối với hệ thống mạng, Và chiến lược bạn sử dụng trong việc bảo mật những thiết bị điểm cuối này được gọi là bảo mật điểm cuối.

Endpoint security không giống như antivirus

Mặc dù mục tiêu của các giải pháp bảo mật điểm cuối đều là như nhau, tức là giữ cho một thiết bị được an toàn, nhưng vẫn có sự khác biệt đáng kể giữa bảo mật điểm cuối và phần mềm chống virus. Antivirus chú trọng hơn vào việc bảo vệ các PC (một hoặc nhiều tùy thuộc vào loại phần mềm chống virus đang được triển

khai), trong khi bảo mật đầu cuối "quan tâm" đến toàn bộ các thiết bị đầu cuối có liên quan nói chung.

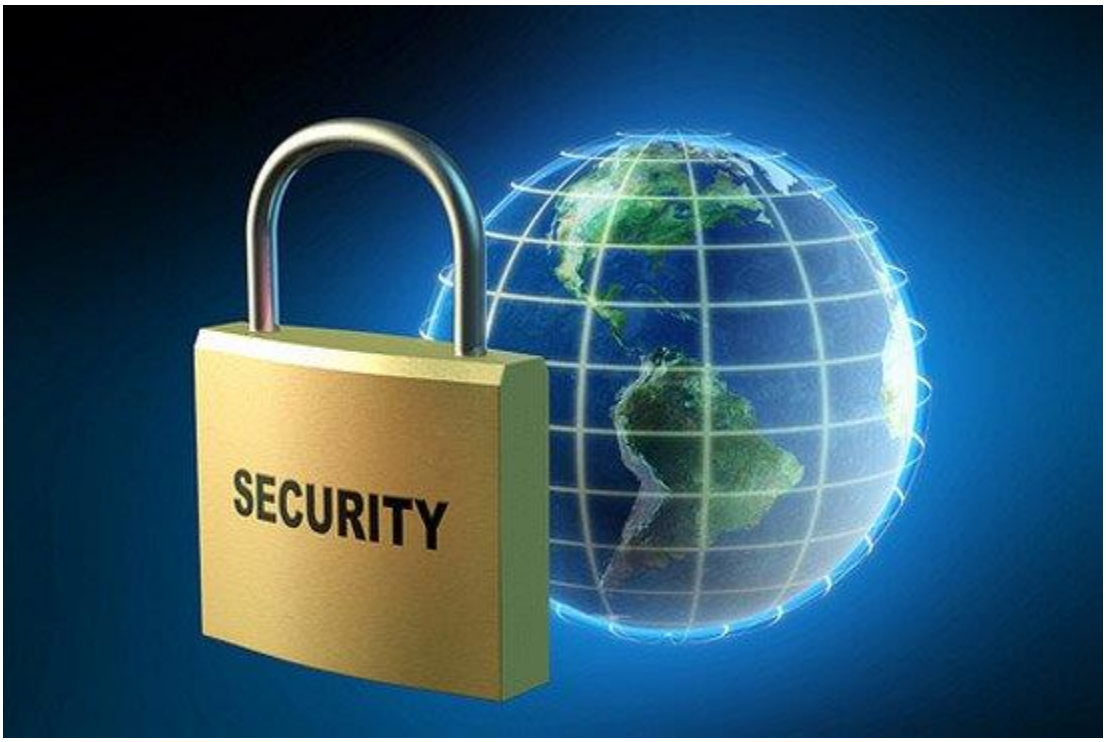


Antivirus là một trong những thành phần của bảo mật điểm cuối. Trong khi đó bảo mật điểm cuối là một khái niệm rộng hơn bao gồm không chỉ chống virus mà còn nhiều công cụ bảo mật (như Firewall, hệ thống HIPS, công cụ danh sách trắng, công cụ vá và ghi nhật ký...) để bảo vệ các thiết bị đầu cuối khác nhau của doanh nghiệp (và bản thân doanh nghiệp) chống lại các các loại mối đe dọa bảo mật đa dạng. Đây cũng là những thứ thường không có sẵn trong các phần mềm chống virus.

Chính xác hơn, bảo mật thiết bị đầu cuối sử dụng mô hình máy chủ/ứng dụng khách để bảo vệ các thiết bị đầu cuối khác nhau của doanh nghiệp. Máy chủ sẽ có một bản ghi chính của chương trình bảo mật và các máy khách (các thiết bị đầu cuối) sẽ có các "tác nhân" được cài đặt bên trong. Các tác nhân này sẽ liên lạc và cung cấp cho máy chủ hoạt động và trạng thái của các thiết bị tương ứng như sức khỏe của thiết bị, xác thực/ủy quyền người dùng... và do đó, giúp giữ an toàn cho thiết bị đầu cuối.

Trong khi đó, phần mềm chống virus thường chỉ là một chương trình duy nhất chịu trách nhiệm quét, phát hiện và diệt virus, phần mềm độc hại, phần mềm quảng cáo, phần mềm gián điệp… Nói một cách đơn giản, antivirus là một công cụ phù hợp để bảo vệ hệ thống mạng gia đình của bạn và bảo mật điểm cuối phù hợp để bảo mật cho các doanh nghiệp lớn hơn và phức tạp hơn nhiều trong xử lý. Cũng có thể nói rằng các phần mềm chống virus là các hình thức bảo mật điểm cuối đơn giản cũng không sai.

Sự khác biệt giữa bảo mật điểm cuối và bảo mật mạng

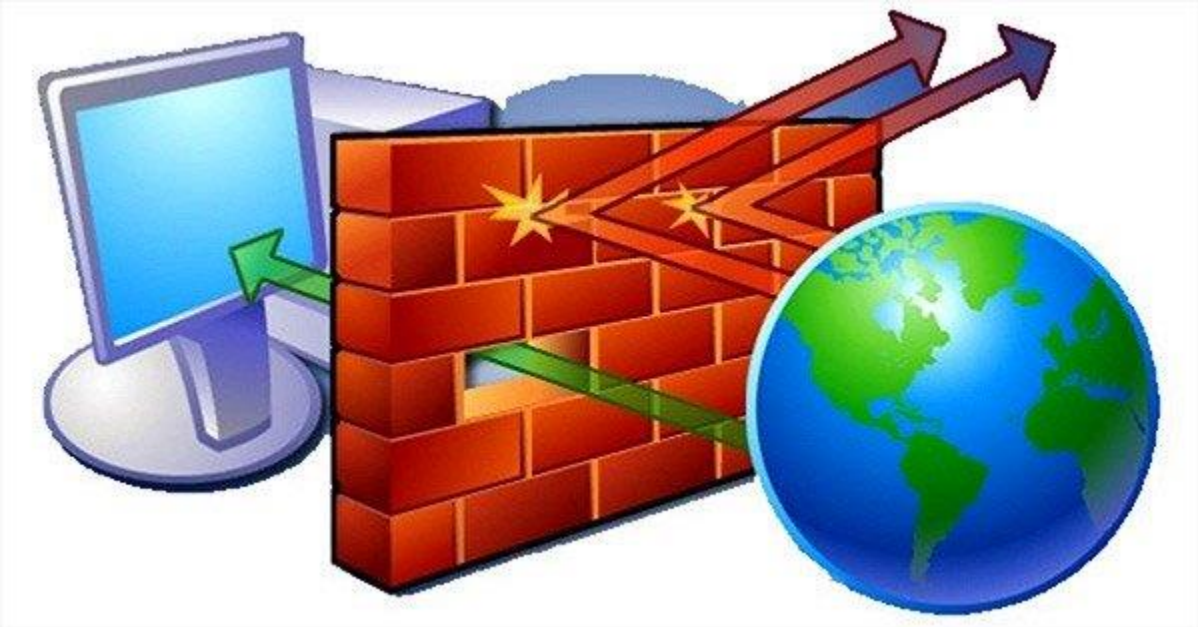


Như đã nói, bảo mật điểm cuối hướng tới việc bảo vệ các thiết bị đầu cuối của doanh nghiệp (thiết bị di động như máy tính xách tay, điện thoại thông minh và nhiều thứ khác), và tất nhiên, doanh nghiệp cũng sẽ chống lại các mối nguy hiểm do các thiết bị đầu cuối này tạo ra. Trong khi bảo mật mạng chú trọng đến việc thực hiện các biện pháp bảo mật để bảo vệ toàn bộ hệ thống mạng của bạn (toàn bộ cơ sở hạ tầng CNTT) để chống lại các mối đe dọa bảo mật khác nhau.

Sự khác biệt chính giữa bảo mật điểm cuối và bảo mật mạng là bảo mật điểm cuối tập trung vào việc bảo mật thiết bị đầu cuối, trong khi đối với bảo mật mạng, trọng tâm lại là bảo vệ hệ thống mạng. Cả hai loại hình bảo mật này đều rất quan trọng. Tốt nhất là chúng ta nên bắt đầu từ việc xây dựng hệ thống bảo mật điểm cuối và

sau đó là hệ thống bảo mật mạng. Có thể hiểu một cách đơn giản, hệ thống mạng của bạn sẽ được an toàn chỉ khi các điểm đầu cuối của bạn được bảo mật chặt chẽ từ trước. Bạn nên lưu ý điều này trước khi bắt đầu tìm kiếm các sản phẩm bảo mật mạng và bảo mật đầu cuối.

Sự khác biệt giữa bảo mật điểm cuối và tường lửa



Tường lửa sẽ chịu trách nhiệm lọc lưu lượng truy cập vào và ra khỏi hệ thống mạng của bạn dựa trên "một bộ quy tắc bảo mật", ví dụ như hạn chế lưu lượng truy cập chảy vào hệ thống mạng từ một trang web chứa những nguy hiểm tiềm ẩn cụ thể. Trong khi bảo mật điểm cuối không chỉ quan tâm đến việc lọc mạng mà còn thực hiện nhiều tác vụ khác như vá, ghi nhật ký và giám sát... để bảo vệ các thiết bị đầu cuối.

Cả chống virus và tường lửa là những yếu tố quan trọng trong bảo mật điểm cuối. Mục tiêu của chúng vẫn được giữ nguyên, mặc dù mô hình áp dụng (mô hình máy khách/máy chủ) và số lượng máy tính mà chúng bảo vệ là khác nhau, và trong mô hình bảo mật điểm cuối, khi hoạt động với các công cụ bảo mật khác nữa, chúng trở sẽ nên hiệu quả hơn rất nhiều.

Bảo mật điểm cuối cũng có nhiều hình thức khác nhau

Tùy theo những tiêu chí về người tiêu dùng và doanh nghiệp mà chúng ta cũng có nhiều hình thức bảo mật điểm cuối khác nhau. Nhìn chung, các giải pháp bảo mật

điểm cuối có thể được chia thành 2 loại khác nhau. Một cho người tiêu dùng và một cho các doanh nghiệp. Sự khác biệt lớn nhất giữa hai loại hình này là đối với người tiêu dùng thì sẽ không có quản lý và quản lý tập trung, trong khi đó, đối với các doanh nghiệp, quản lý tập trung là rất cần thiết. Trung tâm quản trị (hoặc máy chủ) sẽ sắp xếp các cấu hình một cách hợp lý hoặc cài đặt phần mềm bảo mật điểm cuối trên các thiết bị đầu cuối riêng lẻ, sau đó nhật ký về hiệu suất và các cảnh báo khác sẽ được gửi đến máy chủ quản trị trung tâm để đánh giá và phân tích.

Những giải pháp bảo mật đầu cuối này thường chứa những gì?

Mặc dù chắc chắn không có bất kỳ giới hạn nào về các ứng dụng của bảo mật điểm cuối, và danh sách các ứng dụng này sẽ còn được mở rộng thêm trong tương lai, nhưng vẫn sẽ có một số ứng dụng cốt lõi cho bất kỳ giải pháp bảo mật điểm cuối nào.

Một số ứng dụng này có thể kể đến như tường lửa, các công cụ chống virus, công cụ bảo mật internet, công cụ quản lý thiết bị di động, mã hóa, công cụ phát hiện xâm nhập, giải pháp bảo mật di động…

Bảo mật điểm cuối hiện đại và truyền thống

Để chỉ rõ những sự khác biệt thực sự giữa bảo mật điểm cuối hiện đại và truyền thống khá là phức tạp vì nó liên tục được thay đổi. Trong khi các doanh nghiệp thường rất miễn cưỡng và ngại thay đổi, ngay cả khi sự thay đổi đó là có lợi cho họ. Thế nhưng bảo mật điểm cuối là một lĩnh vực mà các doanh nghiệp sẽ không có lựa chọn nào khác ngoài việc phải áp dụng những biện pháp an ninh điểm cuối hiện đại nhất. Bởi vì an ninh điểm cuối không chỉ là một công cụ chống phần mềm độc hại mà nó còn có thể tiến những bước dài trong việc bảo vệ hệ thống mạng của các doanh nghiệp chống lại những mối đe dọa bảo mật đang không ngừng được biến đổi mỗi ngày.

Windows 10 và bảo mật điểm cuối

Windows 10 mặc dù được tuyên bố là hệ điều hành Windows an toàn nhất, nhưng vẫn chứa đựng một số điểm yếu về bảo mật. Các chuyên gia bảo mật đã chứng minh rằng các tính năng bảo mật tích hợp của Windows như Windows Defender, Firewall... cũng đang dần trở nên không hiệu quả trong tình hình an ninh phức tạp và không ngừng biến đổi như hiện nay. Do đó các doanh nghiệp sử dụng hệ điều hành Windows 10 vẫn sẽ cần đến bảo mật điểm cuối để bảo vệ các thiết bị đầu cuối khác nhau kết nối với mạng và để bảo vệ chính hệ thống mạng của họ.

Các hệ thống bảo mật được tích hợp sẵn trên Windows sẽ không bao giờ là đủ. Bởi vì các cách thức tấn công an ninh của ngày hôm nay là quá đa dạng và được biến đổi quá nhanh. Điều đó có nghĩa là chúng ta không còn sống trong một thế giới mà nơi các tệp đính kèm email hoặc được tải xuống trên web là các nguồn lây nhiễm phần mềm độc hại duy nhất nữa. Nói một cách đơn giản, hệ điều hành windows của bạn cần thêm các lớp bảo vệ dưới dạng chống virus cho Windows hoặc nhiều hơn nữa nếu có thể tùy thuộc vào yêu cầu của bạn.

Với suy nghĩ đó, chúng ta hãy cùng xem các cách mà bạn có thể bảo vệ hệ điều hành Windows của mình khỏi các mối đe dọa bảo mật khác nhau:

- Giữ cho hệ điều hành Windows của bạn luôn cập nhật phiên bản mới nhất: Hôm nay là Windows 10 nhưng ngày mai sẽ có một phiên bản mới. Dù bất cứ lý do gì đi chăng nữa, hãy đảm bảo rằng PC của bạn luôn được cập nhật

lên phiên bản mới nhất. Đây có lẽ là một trong những biện pháp đơn giản nhất mà bạn có thể làm ngoài việc cài đặt thêm các phần mềm chống virus, bởi vì bản cập nhật mới nhất thường là bản cập nhật sẽ giúp bảo vệ người dùng khỏi tất cả các lỗ hổng bảo mật đã được phát hiện.

- Đảm bảo các ứng dụng khác được cập nhật đầy đủ: Một trong những thành phần quan trọng trong một hệ thống máy tính chính là các ứng dụng. Hãy đảm bảo tất cả ứng dụng trong hệ thống của bạn đều được cập nhật và chứa các bản vá bảo mật mới nhất, bởi vì có một thực tế rõ ràng là các tin tặc thường cố gắng khai thác lỗ hổng tới từ các phần mềm phổ biến như Java, Adobe Flash, Adobe Acrobat… rồi qua đó xâm nhập vào hệ thống của bạn.
- Sử dụng giải pháp bảo mật chủ động: Thật không may một mình các phần mềm chống virus truyền thống sẽ là không đủ trong tình hình hiện nay, đặc biệt là khi bạn đang phải chống lại những phần mềm độc hại hiện đại, sử dụng các phương pháp tinh vi hơn trước rất nhiều. Do đó để giải quyết vấn đề các mối đe dọa an ninh mạng luôn thay đổi, người dùng sẽ phải cần đến các giải pháp bảo mật chủ động như bảo mật Internet (cho quy mô gia đình) và bảo mật điểm cuối (dành cho doanh nghiệp).
- Sử dụng tài khoản cục bộ thay vì tài khoản Microsoft: Nếu bạn đang sử dụng Windows 10, tốt nhất bạn nên tránh sử dụng các tài khoản Microsoft và thay vào đó chọn một tài khoản cục bộ, vì sử dụng tài khoản Microsoft có nghĩa là bạn đã đưa một số thông tin cá nhân của mình lên đám mây và đây không phải là cách hay trong bảo mật. Để chọn một tài khoản cục bộ, hãy truy cập vào Settings > Accounts > Your info và chọn “Sign in with a local account”.
- Đảm bảo kiểm soát tài khoản người dùng luôn được bật: UAC (User Account Control - Kiểm soát tài khoản người dùng) là một biện pháp bảo mật của Windows, chịu trách nhiệm chính trong việc ngăn chặn các thay đổi trái phép (được khởi xướng bởi ứng dụng, người dùng, virus hoặc các dạng phần mềm độc hại khác) đối với hệ điều hành. UAC sẽ đảm bảo các thay đổi sẽ chỉ được áp dụng cho hệ điều hành khi có sự chấp thuận của quản trị viên hệ thống. Do đó hãy luôn bật tính năng này.
- Thực hiện các hoạt động sau lưu thông thường: Hãy luôn chuẩn bị sẵn sàng cho những tình huống “tệ nhất” khi nói đến việc đối phó với các mối đe dọa

bảo mật, đó là hệ thống của bạn bị mất kiểm soát hoàn toàn. Do đó, hãy thực hiện sao lưu thường xuyên đối với hệ thống của bạn (cả trực tuyến và ngoại tuyến) để tất cả dữ liệu sẽ không bị mất trong trường hợp máy tính của bạn bị ảnh hưởng nặng nề bởi các mối đe dọa bảo mật hoặc gặp sự cố không thể khắc phục về phần cứng.

- Cập nhật trình duyệt của bạn thường xuyên: Trình duyệt là những gì chúng ta sử dụng để truy cập Internet. Do đó, các lỗ hổng bảo mật trong trình duyệt cũng có nghĩa là con đường để các các mối đe dọa bảo mật "nhập cảnh" vào hệ thống của bạn cũng trở nên rộng mở hơn. Do đó, cũng giống như với hệ điều hành và các ứng dụng khác, hãy luôn cập nhật trình duyệt web của bạn lên những phiên bản mới nhất. Các biện pháp bảo mật khác bạn có thể thực hiện đối với trình duyệt: 1) Chọn chế độ duyệt web riêng tư để ngăn các chi tiết nhạy cảm được lưu trữ. 2) Ngăn chặn hoặc chặn cửa sổ bật lên. 3) Cấu hình cài đặt bảo mật trình duyệt web để cải thiện bảo mật…

- Tắt tính năng theo dõi vị trí: Nếu bạn đang sử dụng Windows 10 hoặc bất kỳ phiên bản nào khác có chứa tính năng theo dõi vị trí (Location Tracking) thì tốt nhất là bạn nên tắt nó đi hoặc chỉ sử dụng khi thực sự cần thiết. Ví dụ: nếu bạn muốn biết các thông tin về thời tiết tại nơi mình sống hoặc các cửa hàng khác nhau gần đó… Để tắt theo dõi vị trí, hãy truy cập vào Privacy > Location nhấp vào nút Change và sau đó di chuyển thanh trượt từ On sang Off.

- Sử dụng Internet một cách khôn ngoan hơn: Tất cả các biện pháp bảo mật được liệt kê ở đây sẽ trở nên vô ích nếu bạn không thận trọng khi hoạt động trên mạng. Do đó, hãy đảm bảo rằng bạn không nhấp vào liên kết tìm kiếm nguy hiểm, tải xuống những tệp đính kèm độc hại từ email không xác định hoặc từ các trang web không đáng tin cây, cũng như tránh truy cập vào các trang web đáng ngờ…

Hệ điều hành Windows có lẽ là một trong những hệ điều hành tốt nhất hiện nay, và đó cũng là lý do tại sao nó trở nên rất phổ biến và được sử dụng rộng rãi trên toàn thế giới mặc dù vẫn còn chứa đựng một số mối đe dọa về an ninh. Công bằng mà nói thì chẳng có hệ điều hành nào là an toàn tuyệt đối cả, vấn đề nằm ở chỗ chỉ cần đảm bảo rằng bạn có thể tự trang bị cho mình những kiến thức cần thiết về bảo mật

cũng như sử dụng các sản phẩm bảo mật phù hợp và tuân thủ các phương pháp bảo mật tốt nhất. Làm được những điều này sẽ đảm bảo hệ điều hành Windows của bạn luôn được an toàn cho dù trong bất cứ tình huống nào.

Chúc các bạn xây dựng được cho mình một hệ thống bảo mật tuyệt vời!