Kingston TECHNOLOGY

Thiết bị lưu trữ USB: Mã hóa phần cứng có ngăn chặn được rủi ro hay không?

#KingstonIsWithYou

Thiết bị lưu trữ USB: Mã hóa phần cứng có ngăn chặn được rủi ro hay không?

Lời nói đầu và nội dung

Hơn bất kỳ lúc nào khác, an ninh mạng đang là mối quan tâm hàng đầu ở các doanh nghiệp, nhưng thực tế là vẫn còn rất nhiều công ty chưa hiểu rõ và không chuẩn bị đủ để đối phó với các mối đe dọa. Theo UpCity, tại Hoa Kỳ, chỉ có 50% doanh nghiệp có sẵn kế hoạch đảm bảo an ninh mạng. Trong số đó, có đến 32% chưa hề cập nhật kế hoạch này từ đầu đại dịch COVID-19 – đây là giai đoạn nhiều doanh nghiệp chuyển sang mô hình làm việc từ xa hoặc kết hợp. Trong khi đó, tần suất các cuộc tấn công mạng lại ngày càng tăng thêm. Tính tổng trên toàn cầu, số lượng doanh nghiệp bị mã độc tống tiền tấn công đã tăng từ 37% vào năm 2020 lên 66% vào năm 2021[1].

Khi an ninh mạng bị xâm phạm, doanh nghiệp sẽ phải chịu hậu quả cực kỳ nghiêm trọng. Ngoài thiệt hại tài chính, thì việc mất dữ liệu, sự an toàn và tổn hại danh tiếng có thể tác động tiêu cực đến doanh nghiệp theo nhiều cách, cả ngắn hạn và dài hạn.

Một loại phương tiện phổ biến mà tội phạm mạng thường sử dụng chính là các ổ USB. Những ổ này đã trở nên phổ biến trong nhiều công ty nhờ vào tính giản tiện – chỉ cần cắm vào máy là đã có thể sử dụng. Tuy nhiên, chính đặc tính đơn giản này lại khiến các ổ USB rất dễ bị xâm phạm.

Kẻ tấn công chỉ cần dùng một ổ USB bị mất hoặc lấy cắp là đã có thể truy cập vào dữ liệu có khả năng là dữ liệu nhạy cảm. Chính lúc này, tính năng mã hóa có thể đóng một vai trò rất lớn biến USB trở thành công cụ an toàn để sử dụng và giúp giảm thiểu mọi rủi ro liên quan cho cá nhân và công ty. Trong sách điện tử này, chúng tôi sẽ giải đáp những thắc mắc chính sau đây:

- Vì sao USB mã hóa lại có vai trò rất quan trọng trong bảo vệ chống lại các cuộc tấn công mạng?
- Đâu là những điểm dễ bị tấn công trong công ty?
- Các công ty có thể làm gì để bảo vệ mình?

Mục lục	Trang

Thiết bị lưu trữ USB: Mã hóa phần cứng có ngăn chặn được rủi ro hay không?

Cộng tác viên

Sách điện tử này được soạn thảo với sự tham gia của các nhân vật đầu ngành về CNTT và công nghệ mới nổi, cùng với chuyên gia kỹ thuật nội bộ của Kingston.

David Clarke

David được Thompson Reuter công nhận là một trong 10 người có tầm ảnh hưởng hàng đầu trong danh sách "Top 30 nhà lãnh đạo và nhà tư tưởng có ảnh hưởng nhất trên mạng xã hội về quản lý rủi ro, tuân thủ và công nghệ đăng ký tại Vương quốc Anh", đồng thời nằm trong danh sách 50 Chuyên gia toàn cầu hàng đầu của Kingston Technology.

Pasi Siukonen

Pasi chịu trách nhiệm dẫn dắt một đội ngũ chuyên gia hỗ trợ các phòng ban của Kingston như PR, Tiếp thị, Bán hàng thị trường, Hỗ trợ kỹ thuật và Dịch vụ khách hàng về các sản phẩm Kingston. Tâm điểm sản phẩm chủ yếu của ông là các dòng sản phẩm ổ Flash và ổ SSD.

Điểm khác biệt giữa ổ thương mại và ổ mã hóa

Nếu ổ thương mại (không mã hóa) rất dễ truy cập và sử dụng, thì tính năng mã hóa phần cứng sẽ bổ sung thêm một số lớp bảo mật – cả về phần cứng lẫn phần mềm – để giúp thiết bị lưu trữ USB trở bảo mật hơn rất nhiều. Với tính phổ biến dễ tiếp cận, giá rẻ và tính di động, các ổ không có mã hóa loại thương mại rất thuận tiện cho người dùng, nhưng đồng thời cũng vô cùng thuận tiện cho những kẻ tấn công muốn đánh cắp dữ liệu nhạy cảm, đưa phần mềm độc hại hoặc mã độc tống tiền vào mạng công ty, v.v. USB được sử dụng rất thường xuyên nên cũng tiềm ẩn nhiều khả năng xảy ra tấn công mạng. Các ổ thương mại đi kèm với hai rủi ro chính:

- **Tấn công bằng mã độc tống tiền:** these các cuộc tấn công dựa trên USB này bao gồm đưa phần mềm độc hại vào mạng công ty, nắm giữ thông tin công ty và/hoặc hệ thống để tống tiền bằng cách mã hóa thông tin/hệ thống đó. Những cuộc tấn công này thường do BadUSB gây ra và đã trở thành loại phần mềm độc hại thường gặp nhất.
- **Mất cắp dữ liệu:** chỉ cần một ổ bị mất, đánh cắp hoặc nằm ngoài tầm giám sát, mà không có biện pháp bảo mật thích hợp, là kẻ tấn công đã có thể dễ dàng truy cập được vào dữ liệu lưu trữ trên ổ – dù đó là thông tin khách hàng, mã nguồn hay dữ liệu nhạy cảm về tài chính và hoạt động.

BadUSB là loại tấn công có thể khai thác lỗ hổng của ổ USB có phần mềm điều khiển không được bảo vệ, sau đó lập trình phần mềm điều khiển bằng phần mềm độc hại. Đối với tội phạm mạng, các công cụ độc hại này cực kỳ phổ biến và dễ dàng có được. Tuy nhiên, do nhận thức về những công cụ này vẫn còn thấp, nên để thực hiện các cuộc tấn công vẫn là chuyện rất dễ dàng, chỉ cần thay thế phần mềm điều khiển của ổ thương mại bằng phần mềm điều khiển đã bị xâm nhập, trong đó ổ USB có thể giả dạng bàn phím và chạy các tập lệnh để tấn công tường lửa. Do có rất nhiều cuộc tấn công mạng được thực hiện thông qua các nhân viên nội bộ có hoặc không có mục đích xấu nên điều cực kỳ quan trọng là các doanh nghiệp phải sử dụng ổ mã hóa với phần mềm điều khiển được bảo vệ và có chữ ký số để ngăn chặn các cuộc tấn công này, giúp giảm cơ hội thành công của tội phạm mạng.

> “Chi phí xây dựng lại cơ sở hạ tầng cũng như trả tiền chuộc và các hành vi tống tiền khác là rất lớn so với chi phí mua các loại ổ USB được quản lý. - David Clarke”

Vì sao chúng ta nên sử dụng USB mã hóa?

Ổ mã hóa được thiết kế đặc biệt để bảo vệ cả dữ liệu chứa bên trong ổ và mọi thiết bị kết nối với ổ, khiến ổ mã hóa trở thành công cụ có giá trị trong kho vũ khí CNTT của mọi công ty. Khi các mối đe dọa an ninh mạng ngày càng tinh vi hơn, thì các tính năng của ổ mã hóa cũng ngày càng tiên tiến, cho phép đi trước bọn tội phạm mạng đang tìm cách khai thác các thiết bị này. Như đã thấy trong dòng sản phẩm mã hóa phần cứng Kingston IronKey™, các tính năng như mã hóa AES 256 bit ở chế độ XTS mạnh nhất, vỏ chống va đập và giả mạo, phần mềm điều khiển có chữ ký số, bàn phím ảo, chế độ mật khẩu phức tạp hoặc cụm mật khẩu, v.v. đã được phát triển và thêm vào qua các năm để bảo vệ thật toàn diện và chắc chắn cho người dùng trước mọi hình thức tấn công.

Vì thường không hiểu rõ về rủi ro mạng nên nhiều doanh nghiệp sẽ chọn sử dụng các ổ thương mại, dù các ổ này có rất nhiều lỗ hổng. Một lý do quan trọng cũng là do tính phổ biến dễ tìm, giá rẻ và việc sử dụng mã hóa phần mềm, cũng như do thiếu quy trình phê duyệt ổ flash của công ty. Rất nhiều công ty không có chính sách hoặc quy trình thực hành tốt nhất để tuân thủ các tiêu chuẩn CNTT và an ninh mạng khác nhau, chẳng hạn như các quy tắc thực hành ISO27001, GDPR, SOC2 và WISP của chính phủ. Điều này cũng có nghĩa là rủi ro thường được đánh giá dựa trên quan điểm thay vì bằng chứng – khiến nhiều công ty dễ bị tấn công.

Dù cũng có công ty sử dụng ổ thương mại cùng với các công cụ mã hóa phần mềm hiện có, nhưng đây thường là cách tiết kiệm sai lầm vì bất kỳ ai cũng có thể sử dụng các công cụ miễn phí hoặc trả phí trên Internet để tấn công các ổ mã hóa phần mềm. Hơn nữa, khi muốn thuận tiện hoặc để sử dụng trên nền tảng hệ điều hành không được hỗ trợ, người dùng vẫn có thể xóa tính năng mã hóa phần mềm ra khỏi ổ bằng một thao tác đơn giản là định dạng lại ổ. Ngược lại, USB mã hóa phần cứng là lựa chọn phù hợp hơn nhờ có tính năng mã hóa luôn bật và không thể tắt được. Cùng với đó là thiết kế chống giả mạo, niêm phong chống mở hộp và sử dụng phần mềm điều khiển có chữ ký số để đảm bảo tính xác thực và toàn vẹn của ổ. Giới hạn số lần nhập mật khẩu (bảo vệ chống tấn công Brute Force) và bàn phím ảo (bảo vệ chống theo dõi bàn phím và theo dõi màn hình) là hai tính năng khác của ổ mã hóa như IronKey VP50, nghĩa là ổ này tuân thủ các quy tắc thực hành tốt nhất trong ngành để chống lại tác nhân độc hại muốn trích xuất mật khẩu từ những người dùng.

> Nếu ổ IronKey phát hiện ra phần mềm điều khiển đã bị giả mạo, ổ sẽ đóng lại và không khởi động,từ đó tăng cường an ninh mạng. - Pasi Siukonen

Ai sẽ gặp phải rủi ro?

Trên thực tế, bất kỳ công ty nào không thể kiểm soát được quyền truy cập USB của mình đều có rủi ro – và thông thường, họ không biết chính xác những rủi ro đó là gì. Tuy nhiên, có những yếu tố có thể khiến một số công ty trở thành mục tiêu hấp dẫn – và dễ bị tấn công hơn – trước các cuộc tấn công mạng.

Dữ liệu của các công ty trong lĩnh vực chăm sóc sức khỏe và tài chính không chỉ thu hút hơn nhiều đối với tội phạm mạng, mà còn tác động đến cả tổ chức và khách hàng theo những chiều hướng nghiêm trọng hơn. Vào năm 2017 tại Vương quốc Anh, một cuộc tấn công mạng nhắm vào tổ chức NHS (Dịch vụ Y tế Quốc gia) đã khiến hơn 19.000 cuộc hẹn bị hủy và khiến NHS thiệt hại 92 triệu bảng Anh vì thất thoát hiệu suất, cũng như chi phí khôi phục dữ liệu và hệ thống. Sự kiện này không chỉ khiến các bệnh nhân bị ảnh hưởng không được chăm sóc sức khỏe, mà còn khiến NHS bị chỉ trích nặng nề vì phản ứng không kịp thời hoặc không đủ trước các cảnh báo về mối đe dọa mạng trước đó. Dù mọi doanh nghiệp đều cần cập nhật và có đầy đủ thông tin về an ninh mạng, nhưng những tổ chức xử lý thông tin nhạy cảm – đặc biệt là dữ liệu thuộc hạng mục đặc biệt – cần phải thận trọng gấp đôi trước rủi ro mạng.

Giá trị công ty tính theo doanh thu càng cao thì lợi ích mà những kẻ tấn công thu được càng lớn – do đó, rủi ro mà công ty phải đối mặt từ các mối đe dọa mạng cũng lớn hơn. Tuy nhiên, điều đó không có nghĩa là các công ty nhỏ không cần lo lắng về an ninh mạng. Dù các tập đoàn có thể là mục tiêu tấn công hấp dẫn hơn, nhưng họ cũng thường có nguồn lực và nhân viên chuyên trách để giải quyết các mối đe dọa mạng. Trái lại, nhiều doanh nghiệp vừa và nhỏ không có đội an ninh mạng chuyên trách. Các giám đốc điều hành cấp cao của họ lại thường được đưa vào ngoại lệ không phải quản lý USB, khiến các doanh nghiệp này rất dễ bị tấn công với hậu quả cực kỳ nghiêm trọng. Một số nghiên cứu cho thấy thật ra các doanh nghiệp vừa và nhỏ mới là mục tiêu thường bị nhắm đến hơn trong các cuộc tấn công mạng.

Rủi ro đối với nhân viên ở vị trí điều hành cấp cao thậm chí còn lớn hơn nữa. Những cá nhân này dễ dàng bị theo dõi và thường có đặc quyền điều hành trong công ty, nghĩa là các biện pháp kiểm soát mạng – chẳng hạn như quy trình quản lý USB – không áp dụng với họ, khiến họ trở thành mục tiêu béo bở cho bọn tội phạm mạng. Chính lúc này, việc dùng các ổ có tính năng mã hóa phần cứng luôn bật, trang bị đầy đủ thông tin về an ninh mạng, cũng như tuân theo các quy trình và quy tắc thực hành tốt nhất – tất cả có thể giúp giảm đáng kể rủi ro cho doanh nghiệp và bảo vệ hữu hiệu trước các cuộc tấn công.

> Trong số các vụ vi phạm gần đây, có nhiều vụ được kẻ tấn công thực hiện bằng cách sử dụng trợ giúp từ nội bộ, dù vô tình hay cố ý. - David Clarke

Ai sẽ gặp phải rủi ro?

> Những điều các công ty đang thực hiện là chưa đủ để chống lại các mối đe dọa an ninh mạng. - David Clarke

Đối với các công ty, chuỗi cung ứng là một điểm dễ bị tấn công khác. Và thực tế là các cuộc tấn công vào chuỗi cung ứng cũng cực kỳ phổ biến. Vào năm 2013, nhà bán lẻ Target của Mỹ đã vướng phải một trong những vụ vi phạm dữ liệu lớn nhất trong lịch sử bán lẻ, làm lộ thông tin thẻ ghi nợ và thẻ tín dụng của hơn 40 triệu khách hàng. Trên thực tế, Target cũng đã rất chú trọng đến vấn đề an ninh mạng và vừa mới cài đặt một hệ thống an ninh mạng mở rộng 6 tháng trước khi xảy ra vụ việc. Tuy nhiên, những kẻ tấn công đã thâm nhập vào một trong những nhà cung cấp bên thứ ba của Target và qua đó lấy được quyền truy cập vào mạng dữ liệu chính của họ. Tổng cộng đã có 90 vụ kiện chống lại Target và công ty đã mất 61 triệu đô la để dàn xếp vụ vi phạm. Dù có thể Target không chịu trách nhiệm trực tiếp về cuộc tấn công này, nhưng điểm yếu trong hệ thống an ninh mạng của chuỗi cung ứng đã đủ để gây thiệt hại về cả tài chính lẫn danh tiếng.

Giải pháp đường vòng của nhân viên cũng có thể là nguồn tạo lỗ hổng. Tuy những giải pháp đường vòng này có thể giúp nhân viên làm việc hiệu quả hơn trong công việc hàng ngày, nhưng các quy trình bảo mật cơ bản và các quy tắc thực hành tốt nhất lại thường bị bỏ qua, chẳng hạn như quản lý mật khẩu. Mặc dù hướng dẫn từ NCSC và CISA khá đơn giản nhưng việc triển khai trên thực tế thường khó hơn, đặc biệt đối với các thành viên không thành thạo CNTT và an ninh mạng trong nhóm. Có thể nói sở hữu nhóm bảo mật không gian mạng chuyên trách chắc chắn sẽ có ích, nhưng nếu cung cấp cho nhân viên công cụ phù hợp – chẳng hạn như ổ mã hóa phần cứng – thì sẽ giúp giảm đáng kể rủi ro từ giải pháp đường vòng mà họ hay thực hiện.

> Các ổ USB mã hóa phần cứng ngày nay rất dễ sử dụng và tích hợp vào chính sách an ninh mạng hiện có của tổ dụng. Các ổ này có nhiều loại giao diện (đồ họa, bàn phím, màn hình cảm ứng), hỗ trợ nhiều hệ điều hành và có nhiều mức dung lượng để đáp ứng mọi nhu cầu của công ty. - Pasi Siukonen

Các công ty có thể làm thế nào để giảm nguy cơ tấn công mạng?

Các công ty và tổ chức có thể thực hiện một số phương pháp để bảo mật điểm cuối và bảo vệ dữ liệu. Nếu không triển khai chiến lược GRC (Quản trị, Rủi ro, Tuân thủ) thì an ninh mạng chắc chắn sẽ bị phá vỡ. Do đó, việc làm quen và tuân theo các quy trình là vô cùng quan trọng để các doanh nghiệp tự bảo vệ mình. Triển khai phần mềm bảo mật điểm cuối mạnh mẽ cũng có thể vô hiệu hóa một số mối đe dọa mạng. Đồng thời, hãy phản ứng nhanh nhất có thể khi cần vá các lỗ hổng bảo mật.

> Quyết định có áp dụng chính sách mã hóa bắt buộc hay không cũng là một bài toán quan trọng không kém hoặc thậm chí còn quan trọng hơn trong quản lý rủi ro. Lý do là vì vấn đề này sẽ quyết định liệu bạn có sao lưu dữ liệu của mình hay không.
>
> - Pasi Siukonen

Tuy nhiên, ở cấp độ cá nhân, phần cứng mã hóa có thể giúp giảm đáng kể các lỗ hổng, chống lại các mối đe dọa an ninh mạng. Khi các công việc từ xa và kết hợp ngày càng gia tăng và kéo dài, đặc biệt là khi tấn công mạng có xu hướng tăng lên vào năm ngoái, việc đảm bảo rằng nhân viên ở mọi cấp độ của công ty được xử lý, chuyển giao và đọc dữ liệu công ty một cách bảo mật đang trở nên quan trọng hơn bao giờ hết. USB mã hóa phần cứng cho phép người dùng tiếp tục tận dụng tính di động và đơn giản của ổ flash, những vẫn có thể giảm đáng kể rủi ro liên quan đến các ổ này. Nếu làm thất lạc hoặc bị mất cắp ổ thương mại có thể dẫn đến mất dữ liệu, tiền bạc, danh tiếng, v.v. thì với ổ mã hóa phần cứng, bạn có thể yên tâm vì chúng được thiết kế để bảo vệ dữ liệu nhạy cảm khỏi hàng loạt các cuộc tấn công. Hơn nữa, khi tội phạm mạng phát triển các cách thức tấn công mới, các ổ mã hóa sẽ tiếp tục phát triển để vượt qua những thách thức mới này.

Nhìn chung, chi phí đối phó với một cuộc tấn công mạng có thể rất lớn. Và trên thực tế, dù việc ứng dụng và sử dụng ổ mã hóa ở cấp độ công ty có thể đòi hỏi phải thiết lập và phê duyệt nhiều hơn, nhưng về lâu dài lại có thể tiết kiệm rất nhiều tiền cho công ty – cả về chi phí khi bị tống tiền và thất thoát doanh thu do tổn hại danh tiếng. Chỉ riêng phí pháp lý của một vụ vi phạm thôi đã cao hơn nhiều so với chi phí đầu tư mua ổ USB mã hóa phần cứng.

> Với cam kết liên tục cung cấp các giải pháp USB mã hóa hiệu quả cao, danh mục sản phẩm của Kingston giúp các công ty đáp ứng mọi cấu hình an ninh mạng – từ mã hóa phần cứng bắt buộc theo tiêu chuẩn ngành, thiết kế tuân thủ chính sách điểm cuối, đến các chức năng quản lý thiết bị.
>
> - Pasi Siukonen

Tóm tắt

Tại Kingston, chúng tôi liên tục quan sát những bước phát triển trong ngành an ninh mạng để đảm bảo rằng ổ mã hóa IronKey của mình luôn theo kịp các yêu cầu mới nhất và đáp ứng nhu cầu an ninh mạng của mọi công ty, dù lớn hay nhỏ. An ninh mạng vẫn đang và sẽ là nỗi lo ngày càng lớn trên toàn cầu, vì vậy, chúng tôi tin tưởng rằng với các công cụ phù hợp và kiến thức sẵn có, các doanh nghiệp có thể trang bị kĩ càng để đối mặt với những thách thức này, bảo vệ cả tổ chức, nhân viên và khách hàng của mình.

Giới thiệu về Kingston

Với hơn 35 năm kinh nghiệm, Kingston có kiến thức để xác định và giải quyết các thách thức về dữ liệu di động – giúp lực lượng lao động của bạn có thể dễ dàng làm việc một cách bảo mật mà không làm tổn hại đến công ty.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021