MÃ HÓA BẰNG PHẦN MỀM VÀ VẤN ĐỀ TUÂN THỦ QUY ĐỊNH: GIẢI PHÁP CHI PHÍ NHỎ CHO CÁC RỦI RO BẢO MẬT LỚN

YÊU CẦU VỀ TÍNH TUÂN THỦ VÀ QUY ĐỊNH

Trước đây, vấn đề bảo mật dữ liệu chỉ được giao cho các bộ phận CNTT, nhưng với việc các vụ vi phạm dữ liệu người tiêu dùng diễn ra với cường độ liên tục, các chính phủ trên toàn thế giới đang đặt ra ngày càng nhiều yêu cầu hơn đối với các doanh nghiệp, quy định mã hóa và bảo mật tất cả dữ liệu có thể dùng để định danh.

Từ đạo luật HIPAA trong lĩnh vực y tế, đến GDPR ở Châu Âu, Trung Đông và Châu Phi và CCPA ở California, các quy định đang áp tính bắt buộc với việc mã hóa các lớp dữ liệu được bảo vệ. Cùng với số lượng tăng vọt về các quy định và các khoản tiền phạt tương ứng cũng như các rủi ro pháp lý, các tổ chức tuân thủ cũng đã tăng theo cấp số nhân trong hơn 3 năm qua.

Do những thay đổi này, các bộ phận CNTT đã rất khó khăn mới bắt kịp được vấn đề bảo mật và chi phí tăng cao. Trong thời gian đại dịch COVID diễn ra, ngân sách đang được phân bổ cho các khoản đầu tư bổ sung vào phần cứng và tường lửa, với chi phí tập trung vào việc mã hóa dữ liệu.

Trên thực tế, có sự gia tăng trong hoạt động mã hóa bằng phần mềm sử dụng Microsoft BitLocker® hoặc phần mềm quản lý điểm cuối của Symantec, McAfee và những công ty khác. Một số doanh nghiệp và người tiêu dùng cũng tận dụng ổ USB tiêu chuẩn từ các nhà cung cấp khác, có tính năng "két" phần mềm.

MÃ HÓA VÀ TRUYỀN DỮ LIỆU

Nhân viên văn phòng và người tiêu dùng thường có nhu cầu mang theo dữ liệu của mình. Họ có thể lựa chọn sử dụng:

1. Dịch vụ điện toán đám mây: Dịch vụ này tiện lợi vì cho phép người dùng truy cập từ bất kỳ thiết bị nào kết nối được với internet. Tuy nhiên, sự linh hoạt lại phải trả giá không nhỏ. Người dùng hoặc công ty sẽ bị loại bỏ quyền kiểm soát dữ liệu khi lưu trữ trên Đám mây, dịch vụ này cũng tiềm ẩn rủi ro khi đã có trường hợp các máy chủ trên Đám mây không được khóa hoặc bị truy cập.
2. Ổ USB tiêu chuẩn: Mặc dù việc mang theo ổ USB có vẻ an toàn hơn, nhưng vẫn có nguy cơ cao bị lộ dữ liệu khi người dùng đánh mất ổ. Ví dụ, nhiều người mang quần áo đi giặt là thường quên USB trong túi, kết quả là các tiệm giặt là thường có ngăn kéo chứa đầy ổ USB, ngoài ra rất nhiều thông tin tối mật được tìm thấy trong các ổ USB bị mất.
3. Ổ USB được mã hóa phần cứng: Các ổ USB này có cấu trúc tùy chỉnh kết hợp bộ điều khiển mã hóa gắn trong và có tính năng kiểm soát truy cập. Dữ liệu nhìn chung được mã hóa bằng cách sử dụng mã hóa trên phần cứng AES-256 bit mạnh nhất ở chế độ XTS, cùng các biện pháp bảo vệ khả thi khác để giảm thiểu các cuộc tấn công dựa trên phần lõi (firmware) và vật lý. Những ổ cứng này do các công ty chuyên về thiết bị bảo mật sản xuất, và dù đắt hơn ổ USB tiêu chuẩn nhưng lại mang đến khả năng bảo mật dữ liệu tốt hơn. Ổ FIPS 197 hoặc FIPS 140-2 Cấp độ 3 có thể tăng thêm mức độ bảo vệ và giúp người dùng an tâm hơn.
4. Ổ USB tiêu chuẩn với tính năng mã hóa bằng phần mềm: Để bảo mật theo quy định, tính năng mã hóa bằng phần mềm có thể được vận dụng thông qua BitLocker hoặc các công cụ khác - đây là những lựa chọn phù hợp nhờ giá tương đối rẻ và cung cấp chế độ mã hóa AES-256 XTS tương tự.

Không ngạc nhiên khi trong hầu hết trường hợp, các doanh nghiệp và ngành nghề có xu hướng chọn phương án thứ 4 là sử dụng ổ USB tiêu chuẩn có tính năng mã hóa bằng phần mềm, chủ yếu vì tính năng này của BitLocker hay các tiện ích két dữ liệu khác thường được cung cấp "miễn phí".

MÃ HÓA BẰNG PHẦN MỀM KHÔNG TUÂN THỦ CÁC QUY ĐỊNH

Với một chuyên gia bảo mật cho doanh nghiệp, việc mã hóa bằng phần mềm có thể mang lại khả năng mã hóa chính xác tương đương với các ổ USB được mã hóa bằng phần cứng đắt tiền hơn. Nhưng đây có phải con đường đúng đắn không? Do vấn đề thắt chặt ngân sách nên các doanh nghiệp đang chuyển sang mã hóa bằng phần mềm cho các mục đích tuân thủ, nhưng lại không ý thức được mặt tối của việc mã hóa dựa trên phần mềm.

Vấn đề của ổ USB được mã hóa bằng phần mềm là gì? Liệu có phải dữ liệu phần còn lại và chuyển tuyến không được mã hóa dựa trên AES-256 XTS? Nhìn chung thì đúng vậy. Vấn đề là: Việc mã hóa bằng phần mềm được coi là "mã hóa có thể gỡ bỏ".

Khoan đã - Có thể gỡ bỏ là sao? Điều đó có nghĩa là một ổ USB được mã hóa bằng phần mềm có thể bị người dùng vô hiệu hóa phần mã hóa?

Câu trả lời là - Đúng. Người dùng có thể xóa tính năng mã hóa bằng phần mềm khỏi ổ USB của mình. Bạn thắc mắc sao họ làm vậy ư? Vì họ có thể - và vì họ chỉ muốn truy cập các tệp mà không cần dùng mật khẩu hoặc đơn giản là họ quên mật khẩu nhưng lại cần sử dụng ổ USB.

CÁCH XÓA TÍNH NĂNG MÃ HÓA BẰNG PHẦN MỀM KHỎI Ổ USB ĐÃ ĐƯỢC MÃ HÓA

Đối với người dùng không muốn mất thời gian cho việc nhập mật khẩu phức tạp hoặc dùng các mật khẩu khác để truy cập dữ liệu của mình, quy trình rất đơn giản:

1. Cắm ổ đã được mã hóa bằng phần mềm vào một máy tính
2. Định dạng ổ đĩa
3. Sau khi ổ đĩa được định dạng, tất cả tính năng mã hóa sẽ bị xóa
4. Sao chép các tệp có thông tin bí mật hoặc bảo mật vào ổ đĩa để dễ dàng truy cập

Người dùng rất dễ thực hiện tác vụ này khi sử dụng một máy tính không bị hạn chế quyền - thông thường, các bộ phận CNTT hạn chế quyền sử dụng lệnh định dạng trên máy tính của công ty, nhưng việc định dạng ổ có thể được thực hiện trên bất kỳ máy tính nào khác không phải của công ty.

Vì mục đích Tuân thủ – việc xóa mã hóa dữ liệu dễ dàng đồng nghĩa với việc ổ cứng do công ty cung cấp không còn được mã hóa, mặc dù những dữ liệu đã được mã hóa trên ổ này coi như đã mất vĩnh viễn sau khi người dùng xóa bỏ mã hóa bằng phương pháp trên (các khóa mã hóa được liên kết với dữ liệu). Bất kỳ dữ liệu nào được sao chép trên thiết bị sau khi xóa mã hóa được coi là không an toàn và có khả năng không đủ điều kiện tuân thủ, đồng nghĩa với việc có nguy cơ vi phạm các quy định từ HIPAA, GDPR, CCPA và nhiều đạo luật khác.

HẬU QUẢ CỦA VIỆC MẤT Ổ CỨNG KHÔNG ĐƯỢC MÃ HÓA

Trong trường hợp một ổ USB của công ty bị mất và được tìm thấy sau đó, ngay cả khi ban đầu công ty không được biết nhưng sau đó nghe tin qua mạng xã hội, các yêu cầu tuân thủ đặc biệt sẽ được kích hoạt đối với công ty và có thể yêu cầu họ:

1. Tiến hành một cuộc điều tra mang tính pháp lý để xác định loại dữ liệu nào đã bị mất
2. Thông qua sự tham vấn của Bộ phận pháp lý, xác định xem có xảy ra việc vi phạm pháp luật không
3. Xác định xem có cần thông báo cho khách hàng không

Đây là lúc mà tiêu tốn tiền bạc chỉ cho một ổ USB bị mất. Với giá tư vấn pháp lý ở mức hàng trăm đô la một giờ, quy trình tuân thủ này có thể tiêu tốn thêm hàng nghìn đô la khác, bên cạnh các khoản tiền phạt, rắc rối với khách hàng, các vụ kiện cáo khác và sự lúng túng do bị lộ dữ liệu.

Việc mã hóa bằng phần mềm thường được cân nhắc triển khai nhờ chi phí thấp, nhưng những rủi ro đi kèm và hậu quả tài chính to lớn lại không được xem xét.

Khi cho phép sử dụng ổ USB không được mã hóa trên mạng công ty, doanh nghiệp còn đối mặt với một mối nguy khác. Mối nguy này thường được gọi là "BadUSB". BadUSB là một loại phần mềm độc hại từng được những kẻ xấu sử dụng để vượt tường lửa của công ty và đưa phần mềm độc hại vào hệ thống bảo vệ mạng thông qua USB.

BadUSB

Khi một ổ USB được cắm vào máy tính, bộ điều khiển chipset của máy tính bắt đầu hợp tác với bộ điều khiển ổ USB thông qua phần lõi. Việc trao đổi này thậm chí còn xảy ra trước khi Hệ điều hành, như Microsoft/macOS/Linux, nhận biết rằng ổ USB đã được kết nối. Mỗi ổ USB đều có phần lõi hoạt động khi ổ được cắm vào cổng USB.

Thông qua cơ chế hợp tác này, kẻ xấu biết chúng có thể đưa phần mềm độc hại vào máy bằng cách thay thế phần lõi chạy trên ổ USB bằng một phần mềm khác độc hại hơn, đưa phần mềm này vào hệ thống máy tính mục tiêu trong quá trình giao tiếp với ổ USB. Ổ USB tiêu chuẩn không có tính năng bảo mật trên phần lõi bên trong, vì vậy BadUSB ra đời dưới dạng ổ USB tốt đã được trang bị vũ khí để xâm nhập tường lửa và xuyên thủng hệ thống phòng thủ mạng.

Nhiều công ty nỗ lực bảo mật bằng cách cấm sử dụng ổ USB trên hệ thống máy tính của mình, hoặc thậm chí còn bít các cổng USB bằng epoxy. Tuy nhiên, họ nhận thấy nhân viên thuộc các cấp khác nhau đều có nhu cầu mang theo dữ liệu trên ổ USB. Ví dụ: các giám đốc điều hành muốn mang theo dữ liệu để làm việc hoặc cung cấp cho các cố vấn Pháp lý hoặc Tài chính ở bên ngoài, những người không truy cập được vào hệ thống Đám mây của công ty; các nhà thầu của công ty cần dữ liệu để làm việc nhưng bị hạn chế quyền truy cập vào cơ sở dữ liệu; các nhà phân tích tài chính đang gấp rút hoàn thành các báo cáo hàng tháng và cần làm việc trên các bảng tính ở nhà.

Phân tích trước đây cho thấy, có một rủi ro đáng kể khi sử dụng giải pháp mã hóa bằng phần mềm + ổ USB tiêu chuẩn này. Thoạt nhìn, thứ có vẻ rẻ hơn nhưng lại tiềm ẩn rất nhiều tác hại và dẫn tới chi phí đắt đỏ hơn nhiều. Chỉ 2-3 giờ tham khảo ý kiến luật sư về khả năng vi phạm dữ liệu sẽ tiêu sạch mọi khoản tiền tiết kiệm được nhờ việc sử dụng giải pháp rẻ hơn.

Ổ USB ĐƯỢC MÃ HÓA BẰNG PHẦN CỨNG LÀ LỰA CHỌN TỐT NHẤT ĐỂ TUÂN THỦ QUY ĐỊNH

Ổ USB được mã hóa bằng phần cứng là lựa chọn tốt nhất để Tuân thủ quy định

1. Chế độ mã hóa luôn BẬT trên ổ USB được mã hóa dựa trên phần cứng: Người dùng không thể tắt tính năng mã hóa, không thể đặt lại quy tắc mật khẩu (độ dài tối thiểu, độ phức tạp) và không thể tắt tính năng thử lại mật khẩu tự động. Không giống như mã hóa bằng phần mềm thường không chặn được việc đoán mật khẩu liên tục thông qua các cuộc tấn công từ điển bằng phần mềm, các phiên bản mã hóa bằng phần cứng sẽ giới hạn việc thử lại mật khẩu - và khóa dữ liệu khi nhập sai mật khẩu 10 lần hoặc đôi khi thậm chí ít lần hơn. Tính năng này rất an toàn trong thời đại của siêu máy tính.
2. Các ổ đĩa được mã hóa bằng phần cứng sử dụng bộ điều khiển mã hóa cao cấp và kết hợp nhiều tính năng bảo mật: Mặc dù chúng tôi không thường tiết lộ tất cả các biện pháp bảo mật, nhưng có một biện pháp để bảo vệ khỏi BadUSB. Tại nhà máy, khi phần lõi được tải lên các ổ được mã hóa bằng phần cứng, phần lõi này sẽ nhận được chữ ký điện tử và tải. Điều này có nghĩa là, khi các USB được mã hóa này được cắm vào máy tính, trước tiên bộ điều khiển được mã hóa sẽ kiểm tra tính chân thực của phần lõi thông qua chữ ký kỹ thuật số và chỉ thực hiện tải nếu phần lõi vượt qua quá trình xác minh. Bất kỳ sự thay thế nào với phần lõi sẽ khiến ổ đĩa không hoạt động - nghĩa là không còn mối đe dọa.
3. Ổ USB được mã hóa phần cứng có thể có ID sản phẩm (PID) tùy chỉnh được thiết lập cho từng công ty cụ thể: Các ổ cứng cao cấp này có thể chứa một số nhận dạng kỹ thuật số được lập trình để trong trường hợp ổ được cắm vào tường lửa bên trong hoặc bên ngoài của công ty, thì ổ đĩa đó có thể được xác định là ổ do công ty phát hành. Ví dụ: nếu một nhân viên làm mất ổ cứng của công ty và tới cửa hàng bán lẻ mua cái khác giống hệt, ổ mới mua sẽ không được xác thực trên mạng công ty. Tính năng tùy chỉnh này bổ sung thêm một lớp bảo mật khác cho ổ USB.
4. Ổ được mã hóa phần cứng giúp tiết kiệm tiền rất nhanh chóng: Chu kỳ hoàn vốn trở nên ngắn hơn rất nhiều chỉ nhờ việc giảm thiểu và loại bỏ rủi ro..

Kingston là nhà sản xuất ổ USB được mã hóa lớn nhất thế giới, cung cấp các dòng ổ USB với nhiều tính năng và mức giá khác nhau. Liên hệ trực tiếp với Kingston để tìm hiểu cách chúng tôi có thể giúp bạn tuân thủ an ninh tốt nhờ các lựa chọn USB được mã hóa riêng cho giám đốc điều hành, nhân viên, nhà thầu, v.v.