Synology

Bảo vệ tổ chức khỏi ransomware

Người ta dự báo rằng các cuộc tấn công của ransomware sẽ tiêu tốn tổng cộng 8 nghìn tỷ USD của các tổ chức chỉ riêng trong năm 2023.[1] Kế hoạch bảo vệ dữ liệu với các tùy chọn khôi phục nhanh chóng là vô cùng quan trọng để giảm thiểu tác động của ransomware và các hình thức tội phạm mạng khác.

Date Oct 13, 2023

Sao lưu: tuyến phòng thủ cuối cùng khi sự cố xảy ra

Khi dữ liệu bị mất do xóa hoặc cố ý sửa đổi, các bản sao lưu sẽ giúp bạn khôi phục dữ liệu quan trọng, tránh thời gian downtime gây tốn kém. Tận dụng các giải pháp bảo vệ dữ liệu của Synology để thiết kế chiến lược sao lưu cho toàn bộ cơ sở hạ tầng IT.

Bảo vệ toàn diện

Bảo vệ endpoint cũng như các bản backup chính để tạo ra nhiều tấm lưới an toàn cho dữ liệu.

Khôi phục nhanh

Giảm thời gian ngừng hoạt động xuống mức tối thiểu với các tùy chọn khôi phục tức thì khi xảy ra sự cố.

Lưu trữ bất biến

Ngăn chặn các thay đổi trái phép đối với dữ liệu và bản ghi nhanh.

Sao lưu không cần giấy phép

Sao lưu nhiều dữ liệu nhất có thể trong phạm vi lưu trữ cho phép, không có giới hạn hoặc phí ẩn.

Giải pháp bảo vệ tập trung trước ransomware

Hợp nhất các bản sao lưu từ nhóm máy trạm, server, máy ảo và các ứng dụng đám mây. Tối ưu hóa mức tiêu thụ dung lượng lưu trữ và tránh nghẽn băng thông bằng các công nghệ sao lưu gia tăng và sao lưu dữ liệu. https://www.synology.com/dsm/solution/infrastructure

Khối lượng công việc thực tế

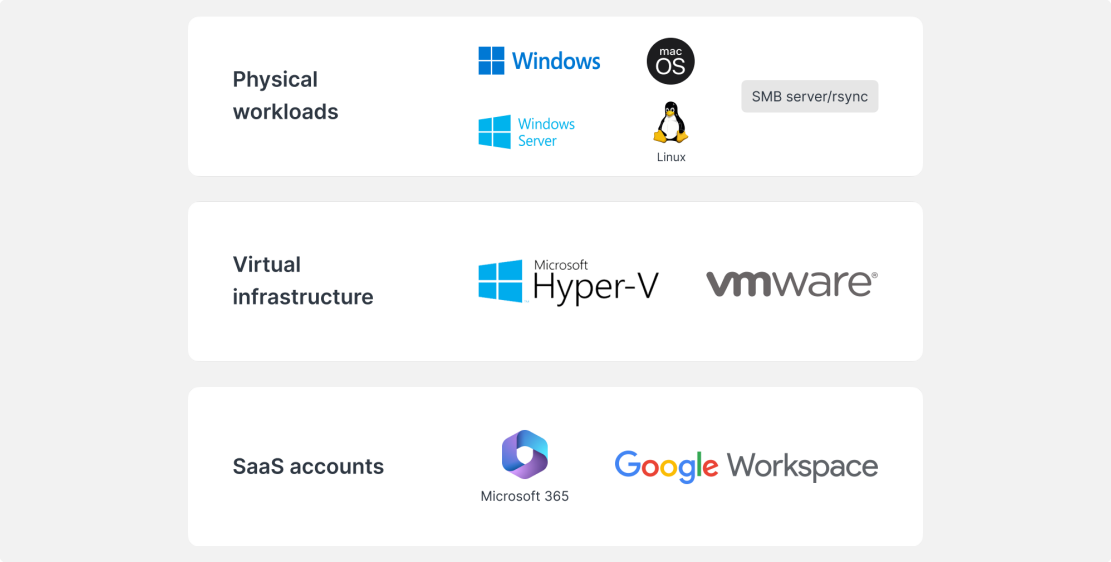
Bảo vệ endpoint trong trường hợp bị tấn công bằng mã độc bằng tính năng sao lưu bare-metal toàn diện và khôi phục linh hoạt từng tập tin.

Cơ sở hạ tầng ảo

Sao lưu máy ảo VMware® vSphere™, Microsoft® Hyper-V® và LUN bằng các công nghệ nén dữ liệu mạnh mẽ.

Tài khoản SaaS

Kích hoạt tính năng bảo vệ liên tục cho dữ liệu lưu trữ trên đám mây, với khả năng tự động phát hiện các tài khoản mới thêm.



Khôi phục hiệu quả

Giảm thiểu thời gian ngưng hoạt động cho các hệ thống sản xuất quan trọng bằng cách nhanh chóng khôi phục các bản sao lưu từ hệ thống Synology tại cơ sở hoặc ngoài cơ sở.

RTO gần bằng không

Gắn bản sao lưu lên VMware®, Hyper-V® hoặc Synology Virtual Machine Manager để tiếp tục công việc nhanh nhất có thể. Khôi phục máy ảo sang một phần mềm giám sát máy ảo thay thế để tránh gián đoạn dịch vụ.

RPO tối thiểu

Thiết lập cấu hình tần suất sao lưu theo nhu cầu, giảm thiểu lượng dữ liệu có khả năng bị ảnh hưởng khi bị tấn công. Bảo vệ hệ thống nhanh chóng nhờ công nghệ sao lưu dữ liệu thay đổi và khử trùng lặp.

Giao diện trực quan

Cho phép nhân viên duyệt và xem trước email, danh bạ và tập tin trên một cổng thông tin thuận tiện trước khi khôi phục, mang lại trải nghiệm thân thiện với người dùng hơn và giảm gánh nặng cho nhóm IT.

Thêm một biện pháp bảo vệ bổ sung

Tuân thủ chiến lược sao lưu 3-2-1 bằng cách lưu trữ bộ dữ liệu thứ ba ngoài cơ sở hoặc trên đám mây, bảo vệ dữ liệu trong trường hợp gặp hỏa hoạn, thiên tai hoặc trộm cắp.

Gửi đến các máy chủ ngoài cơ sở

Lưu trữ các bản sao lưu vào máy chủ Synology tại một vị trí phụ để bảo vệ trước sự cố vật lý và sao chép các bản ghi nhanh bất biến để tăng cường khả năng bảo vệ trước phần mềm tống tiền.

Lên đám mây

Sao lưu vào bất kỳ nhà cung cấp dịch vụ lưu trữ đám mây lớn nào, sử dụng phương thức mã hóa AES-256 phía máy khách để đảm bảo an toàn cho dữ liệu trước hành vi truy cập trái phép. https://c2.synology.com/storage/nas

Được nhiều doanh nghiệp trong ngành tin cậy

“Synology [...] giúp chúng tôi giảm chi phí phần cứng máy chủ [...] đồng thời thực hiện sao lưu cơ sở hạ tầng và máy trạm, lưu nhật ký hệ thống và quản lý tập tin dễ dàng hơn nhiều.”
https://www.synology.com/company/case_study/Investortools

“Nhờ có Active Backup for Business, hiện tại toàn bộ bản sao lưu của chúng tôi đều tập trung và sẵn sàng sử dụng 24/7, giúp chúng tôi giảm thiểu thời gian ngừng hoạt động, đồng thời tuân thủ các quy định của FERPA.”
https://www.synology.com/company/case_study/University_of_Washington

“[...] Active Backup for Business có tốc độ sao lưu đáng kinh ngạc và có khả năng xóa dữ liệu trùng lặp vô cùng hiệu quả, chỉ chiếm 28 TB trong tổng số 58 TB trên máy chủ. [...]”
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

“[...] Active Backup for Business [...] giúp chúng tôi tập trung và quản lý tất cả các tác vụ sao lưu trên một bảng điều khiển duy nhất. Phục hồi nhanh chóng và đáng tin cậy còn giúp đảm bảo tính liên tục của hoạt động kinh doanh.”
https://www.synology.com/company/case_study/UNESCO

Câu hỏi thường gặp

Ransomware là gì?

Ransomware hay mã độc tống tiền là một loại phần mềm độc hại nhằm mã hóa các tập tin của nạn nhân. Sau đó, kẻ tấn công sẽ yêu cầu một khoản tiền chuộc để khôi phục quyền truy cập dữ liệu, thường sẽ đe dọa hủy dữ liệu vĩnh viễn nếu không trả tiền chuộc. Các cuộc tấn công bằng mã độc ransomware có khả năng gây gián đoạn cao và có thể tạo ra tổn thất tài chính đáng kể cho các cá nhân và tổ chức. Bạn cần phải bảo vệ bản thân và thiết bị trước ransomware, chẳng hạn như bằng cách cập nhật phần mềm và thường xuyên sao lưu các tập tin.

Có những loại ransomware nào?

Có nhiều loại mã độc tống tiền ransomware khác nhau và các chủng loại mới liên tục phát triển. Sau đây là một số loại ransomware phổ biến nhất: "

- **Ransomware mã hóa** – Loại ransomware phổ biến nhất này sẽ mã hóa các tập tin để nạn nhân không thể truy cập nếu không có khóa giải mã. Sau đó, kẻ tấn công yêu cầu trả tiền chuộc để đổi lấy khóa
- **Ransomware khóa thiết bị** – Một loại mã độc tống tiền ngăn nạn nhân truy cập máy tính của họ bằng cách thay đổi thông tin xác thực đăng nhập hoặc hiển thị thông báo ngăn nạn nhân truy cập hệ thống. Sau đó, kẻ tấn công yêu cầu trả tiền chuộc để mở khóa máy tính
- **Ransomware dưới dạng dịch vụ (RaaS)** – Một mô hình kinh doanh trong đó kẻ tấn công cung cấp ransomware cho các cá nhân hoặc tổ chức khác muốn thực hiện các cuộc tấn công. Kẻ tấn công thường sẽ cung cấp ransomware và xử lý các khoản thanh toán, còn cá nhân hoặc tổ chức sử dụng dịch vụ sẽ nhận được phần trăm trong khoản tiền chuộc
- **Phần mềm hù dọa Scareware** – Mã độc tống tiền này được thiết kế để dọa nạn nhân trả tiền chuộc. Loại này thường liên quan đến việc hiển thị cảnh báo hoặc thông báo bảo mật giả mạo rằng máy tính của nạn nhân bị nhiễm vi-rút. Sau đó, kẻ tấn công sẽ yêu cầu trả tiền để diệt loại vi-rút không có thực

"

Ransomware lây lan như thế nào?

Ransomware thường lây lan qua email lừa đảo hoặc bằng cách khai thác các lỗ hổng trong hệ thống máy tính. Trong một cuộc tấn công lừa đảo, kẻ tấn công sẽ gửi email giống như đến từ một nguồn uy tín, chẳng hạn như ngân hàng hoặc một công ty nổi tiếng. Email thường chứa liên kết hoặc tập tin đính kèm mà khi nhấp vào, ransomware sẽ cài đặt trên máy tính của nạn nhân. Phương pháp khai thác lỗ hổng trong hệ thống cũng tương tự, ngoại trừ việc kẻ tấn công sẽ sử dụng lỗ hổng bảo mật của hệ thống để cài đặt ransomware mà nạn nhân không hề hay biết. Trong cả hai trường hợp, sau khi cài đặt, ransomware có thể nhanh chóng lây lan sang các máy tính khác trên cùng một mạng.

Quy trình điển hình của một cuộc tấn công ransomware là gì?

Quy trình tấn công ransomware thường theo các bước sau: "

1. Kẻ tấn công giành quyền truy cập vào máy tính của nạn nhân, bằng cách gửi email lừa đảo hoặc bằng cách khai thác lỗ hổng trong hệ thống
2. Khi kẻ tấn công có quyền truy cập vào máy tính của nạn nhân, chúng sẽ cài đặt mã độc ransomware trên hệ thống
3. Sau đó, ransomware sẽ mã hóa các tập tin của nạn nhân, khiến người dùng không thể truy cập được
4. Sau đó, kẻ tấn công sẽ yêu cầu nạn nhân trả tiền chuộc, thường ở dạng tiền kỹ thuật số như Bitcoin, để đổi lấy khóa giải mã nhằm mở khóa các tập tin bị mã hóa
5. Nếu nạn nhân trả tiền chuộc, kẻ tấn công sẽ cung cấp khóa giải mã và nạn nhân sẽ có thể truy cập lại tập tin của mình. Tuy nhiên, không có gì đảm bảo rằng kẻ tấn công sẽ thực sự cung cấp khóa và ngay cả khi họ làm như vậy, các tập tin của nạn nhân có thể bị hỏng hoặc bị lỗi do quá trình mã hóa

" Bạn cần lưu ý rằng có nhiều biến thể trong quy trình này và không phải tất cả các cuộc tấn công ransomware đều tuân theo các bước này một cách chính xác. Ví dụ: một số cuộc tấn công có thể không liên quan đến việc mã hóa tập tin, trong khi những cuộc tấn công khác có thể liên quan đến các hình thức tống tiền hoặc hăm dọa khác.

Tôi bị nhiễm ransomware như thế nào?

Có một số con đường khiến bạn có thể bị nhiễm ransomware. Một trong những cách phổ biến nhất là nhấp vào liên kết độc hại hoặc tập tin đính kèm trong email lừa đảo. Loại email này được thiết kế để trông có vẻ hợp pháp, thường giống email từ một công ty hoặc tổ chức nổi tiếng. Khi bạn nhấp vào liên kết hoặc tập tin đính kèm, chương trình sẽ cài đặt ransomware vào máy tính. Một cách khác có thể khiến bạn bị nhiễm mã độc tống tiền là truy cập trang web bị xâm phạm. Những trang web này đã những kẻ tấn công xâm nhập, chèn mã tự động cài đặt ransomware trên máy tính nếu bạn truy cập trang web. Bạn cũng có thể nhiễm ransomware bằng cách tải xuống các tập tin bị nhiễm độc từ internet. Điều này có thể xảy ra nếu bạn tải xuống tập tin từ trang web đáng ngờ hoặc nếu bạn tải xuống tập tin được chia sẻ bởi người mà bạn không biết. Tóm lại, bạn phải thận trọng khi duyệt internet và tránh nhấp vào liên kết hoặc tải xuống tập tin từ các nguồn lạ. Điều này có thể giúp bảo vệ bạn khỏi bị nhiễm ransomware và các loại phần mềm độc hại khác.

Ai là mục tiêu của ransomware?

Các cuộc tấn công ransomware có thể nhắm mục tiêu vào bất kỳ ai sử dụng máy tính hoặc thiết bị khác được kết nối với internet. Tuy nhiên, một số nhóm đối tượng có nhiều khả năng trở thành mục tiêu hơn những nhóm khác. Ví dụ: các cuộc tấn công ransomware thường nhắm mục tiêu vào các doanh nghiệp, vì họ thường có nhiều dữ liệu có giá trị hơn và có thể sẵn sàng trả tiền chuộc để lấy lại dữ liệu đó. Các bệnh viện, trường học và các tổ chức cung cấp các dịch vụ quan trọng khác cũng là mục tiêu phổ biến, bởi một cuộc tấn công bằng ransomware có thể làm gián đoạn hoạt động của họ và khiến tính mạng của mọi người gặp nguy hiểm. Các cá nhân cũng có thể là nạn nhân tiềm năng của các cuộc tấn công ransomware. Trong những trường hợp này, những kẻ tấn công có thể cố gắng tống tiền nạn nhân bằng cách đe dọa sẽ xóa các tập tin cá nhân của họ hoặc công khai thông tin nhạy cảm nếu không trả tiền chuộc. Mục tiêu của các cuộc tấn công ransomware thường được lựa chọn dựa trên giá trị dữ liệu của họ và khả năng họ sẵn sàng trả tiền chuộc để lấy lại.

Những rủi ro của việc trả tiền ransomware là gì?

Trả tiền chuộc cho kẻ tấn công ransomware có vẻ như là cách dễ dàng nhất để lấy lại các tập tin, nhưng thực tế đó có thể là một quyết định rất mạo hiểm. Có một số rủi ro liên quan đến việc trả tiền chuộc như sau:

- Không có gì đảm bảo rằng kẻ tấn công sẽ thực sự cung cấp khóa giải mã. Trong nhiều trường hợp, nạn nhân trả tiền chuộc không bao giờ nhận được khóa và không thể truy cập tập tin của họ
- Việc trả tiền chuộc có thể khuyến khích những kẻ tấn công tiếp tục chiến dịch tấn công của chúng. Nếu những kẻ tấn công biết rằng nạn nhân sẵn sàng trả tiền chuộc, chúng có thể sẽ thực hiện nhiều cuộc tấn công hơn trong tương lai
- Trả tiền chuộc có thể khiến bạn trở thành mục tiêu cho các cuộc tấn công trong tương lai. Nếu kẻ tấn công biết rằng bạn sẵn sàng trả tiền chuộc, có nhiều khả năng là bạn sẽ trở thành mục tiêu trong tương lai
- Trả tiền chuộc có thể là bất hợp pháp. Trong một số trường hợp, trả tiền chuộc cho một tổ chức tội phạm có thể được coi là một hình thức tài trợ cho khủng bố hoặc các hoạt động bất hợp pháp khác

Mặc dù việc trả tiền chuộc có vẻ như là cách dễ dàng nhất để lấy lại các tập tin, nhưng đó thực sự có thể là một quyết định rất mạo hiểm. Bạn cần phải xem xét cẩn thận các rủi ro trước khi đưa ra quyết định.

Thiệt hại cho ransomware là bao nhiêu?

Thiệt hại của một cuộc tấn công ransomware có thể rất khác nhau tùy thuộc vào một số yếu tố, chẳng hạn như loại ransomware sử dụng, số lượng tập tin bị mã hóa và hiệu quả của cuộc tấn công. Trong một số trường hợp, thiệt hại của một cuộc tấn công ransomware có thể tương đối thấp, trong đó kẻ tấn công yêu cầu khoản tiền chuộc vài trăm đô la. Trong các trường hợp khác, thiệt hại có thể cao hơn nhiều, trong đó kẻ tấn công yêu cầu hàng nghìn đô la hoặc thậm chí nhiều hơn để khôi phục quyền truy cập vào tập tin của nạn nhân. Ngoài các thiệt hại trực tiếp liên quan đến việc trả tiền chuộc, các cuộc tấn công bằng ransomware cũng có thể gây ra các thiệt hại gián tiếp đáng kể. Ví dụ: một cuộc tấn công ransomware có thể tạo ra thời gian ngưng hoạt động và giảm năng suất, dẫn đến mất doanh thu và thu nhập. Các cuộc tấn công này cũng có thể làm tổn hại danh tiếng của công ty và lòng tin của khách hàng, điều này có thể gây ra những tác động tiêu cực lâu dài cho doanh nghiệp. Những thiệt hại gián tiếp này thường cao hơn nhiều so với khoản tiền chuộc.

Các dấu hiệu của ransomware là gì?

Các dấu hiệu của một cuộc tấn công ransomware có thể khác nhau tùy vào loại ransomware cụ thể được sử dụng. Tuy nhiên, một số dấu hiệu phổ biến như sau:

- Các tập tin bị mã hóa và bạn không thể truy cập chúng
- Bạn nhận được tin nhắn từ kẻ tấn công yêu cầu trả tiền chuộc để đổi lấy khóa giải mã
- Bạn thấy các chương trình hoặc tiến trình lạ đang chạy trên máy tính của mình
- Máy tính bị chậm hoặc không phản hồi
- Máy tính hiển thị thông báo lỗi hoặc cửa sổ bật lên bất thường

Nếu bạn nghi ngờ rằng máy tính của mình đã bị nhiễm ransomware, bạn cần phải hành động nhanh chóng. Hãy ngắt kết nối máy tính khỏi internet để ngăn ransomware lây lan.

Làm cách nào để ngăn chặn các cuộc tấn công ransomware?

Có một số bước bạn có thể thực hiện để ngăn chặn các cuộc tấn công của ransomware như sau:

- Sử dụng phần mềm diệt vi-rút hoặc phần mềm bảo mật uy tín và luôn cập nhật phần mềm đó. Phương pháp này có thể giúp bảo vệ máy tính khỏi ransomware và các loại phần mềm độc hại khác
- Hãy thận trọng khi mở các tập tin đính kèm hoặc liên kết email. Ransomware thường được gửi qua email lừa đảo, vì vậy bạn cần phải cẩn thận với những nội dung mà bạn nhấp vào
- Luôn cập nhật hệ điều hành và phần mềm khác. Các bản cập nhật phần mềm thường bao gồm các bản vá bảo mật có thể giúp bảo vệ máy tính khỏi ransomware và các mối đe dọa khác
- Thường xuyên sao lưu tập tin. Phương pháp này có thể giúp bảo vệ dữ liệu nếu máy tính bị nhiễm ransomware. Hãy tuân thủ một trong các chiến lược sao lưu đề xuất, chẳng hạn như chiến lược sao lưu 3-2-1
- Hãy nhận thức về rủi ro của ransomware và hướng dẫn những người khác trong tổ chức về những mối đe dọa này. Phương pháp này có thể giúp ngăn chặn các cuộc tấn công ransomware và giúp dễ dàng phát hiện cũng như ứng phó nếu xảy ra

Cách tốt nhất để ngăn chặn các cuộc tấn công ransomware là luôn cảnh giác và thực hiện các biện pháp để bảo vệ máy tính và dữ liệu. Điều này có thể giúp giảm nguy cơ bị ransomware tấn công và giúp khôi phục dễ dàng hơn nếu xảy ra.

Synology có thể bảo vệ tôi khỏi ransomware như thế nào?

Các biện pháp phòng ngừa là cần thiết để giúp bạn không trở thành nạn nhân của ransomware. Hãy sử dụng các giải pháp Synology sau đây cùng với phần mềm chống vi-rút tùy ý:

- **Ngăn chặn truy cập** – Giảm sự lây lan của ransomware bằng cách đặt tập tin, ứng dụng và quyền truy cập, đồng thời thiết lập cấu hình thông tin xác thực đăng nhập an toàn bằng cách sử dụng Secure SignIn và C2 Password
- **Bảo vệ thiết bị** – Các hệ thống lỗi thời có nguy cơ cao hơn. Hãy cập nhật toàn bộ NAS cùng lúc với Synology Central Management System (CMS) và bảo vệ các thiết bị khác bằng chính sách nhóm trong Synology Directory Server và C2 Identity
- **Tránh các tập tin đáng ngờ** – Thư rác và email lừa đảo có chứa các tập tin đáng ngờ là phương pháp phổ biến để phát tán ransomware. Synology MailPlus mang đến tính năng bảo vệ trước phần mềm độc hại và ngăn chặn thư rác hiệu quả
- **Kiểm tra lỗ hổng bảo mật** – Sử dụng Synology Security Advisor để thường xuyên quét phần mềm độc hại, lỗ hổng bảo mật và các hoạt động đăng nhập bất thường. Tiến hành thay đổi theo đề xuất để cải thiện bảo mật NAS của bạn.
  https://www.synology.com/dsm/overview/security

Các cách khác để bảo vệ dữ liệu của bạn

Quản lý nhóm thiết bị

Tận dụng các tính năng mở rộng để quản lý tập trung quyền truy cập dữ liệu, trạng thái phần mềm, tình trạng hệ thống, v.v.
https://www.synology.com/dsm/overview/administration

Giám sát tất cả các hệ thống

Xác định các hoạt động đăng nhập đáng ngờ, quản lý các bản cập nhật và theo dõi tình trạng của thiết bị, cho dù thiết bị đang đặt ở đâu.
https://www.synology.com/dsm/feature/active-insight

Bảo vệ dữ liệu của bạn

Thực hiện theo quy tắc sao lưu 3-2-1 để bảo vệ dữ liệu khỏi tình trạng vô tình hay cố ý sửa hoặc xóa.
https://www.synology.com/dsm/solution/data_backup

Get started

Contact us

Contact regional sales for more information
https://www.synology.com/form/inquiry/sales

Where to buy

Find a Synology partner in your region
https://www.synology.com/wheretobuy

Lưu ý:

1. eSentire, 2022 Official Cybercrime Report (Báo cáo Tội phạm mạng Chính thức năm 2022) https://www.esentire.com/resources/library/2022-official-cybercrime-report

Bảo vệ tổ chức khỏi ransomware

https://www.synology.com/vi-vn/dsm/solution/ransomware

Trang web Synology

https://www.synology.com/

Liên hệ chúng tôi

https://www.synology.com/company/contact_us