Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Doanh nghiệp nhỏ
Hướng dẫn an ninh mạng

Mức độ Phức tạp của Nội dung
ĐƠN GIẢN ●○○

cyber.gov.au

Giới thiệu

Đối với một doanh nghiệp nhỏ, ngay cả một vấn đề về an ninh mạng nhỏ cũng có thể gây nhiều thiệt hại. Hướng dẫn này bao gồm các biện pháp bảo mật cơ bản để giúp bảo vệ doanh nghiệp của quý vị đối phó với các mối đe dọa an ninh mạng thường gặp. Để bắt đầu, chúng tôi xin gợi ý với ba biện pháp sau đây:

- Bật tính năng xác thực đa yếu tố
- Cập nhật phần mềm của quý vị
- Sao lưu thông tin của quý vị

Hướng dẫn này có thể bao gồm các biện pháp không liên quan đến doanh nghiệp của quý vị, hoặc doanh nghiệp của quý vị có thể có những nhu cầu phức tạp hơn. Sau khi hoàn thành hướng dẫn này, chúng tôi khuyên các doanh nghiệp nhỏ nên áp dụng Mức độ Một của các chiến lược nhằm giảm thiểu vấn đề an ninh mạng trong Tám Mức độ Thiết yếu. Nếu quý vị có thắc mắc về lời khuyên này, hoặc về vấn đề an ninh mạng rộng hơn, chúng tôi khuyên quý vị nói chuyện với chuyên gia Công nghệ Thông tin hoặc một người cố vấn đáng tin cậy.

Truy cập trang cyber.gov.au để đọc hướng dẫn đầy đủ của chúng tôi, bao gồm cả lời khuyên về cách thực hiện cho từng biện pháp.

Mục lục

Các mối đe dọa đối với các doanh nghiệp nhỏ

Tin nhắn lừa đảo

Lừa đảo là cách phổ biến mà tội phạm mạng nhắm vào các doanh nghiệp nhỏ. Mục đích của họ là lừa đảo quý vị hoặc nhân viên của quý vị để:

- gửi tiền hoặc thẻ quà tặng
- nhấp chuột vào các đường dẫn hoặc tập hồ sơ đính kèm độc hại
- tiết lộ thông tin nhạy cảm, chẳng hạn như mật mã.

Tội phạm mạng có thể thử và lừa đảo doanh nghiệp của quý vị qua email, tin nhắn, cuộc gọi điện thoại và mạng xã hội. Họ thường giả danh là một người hoặc tổ chức mà quý vị tin tưởng.

Tấn công qua hình thức lừa đảo

Mối quan tâm đặc biệt đối với các doanh nghiệp nhỏ là **các cuộc tấn công dưới hình thức lừa đảo**. Những trò gian lận này thường chứa một đường dẫn đến một trang mạng giả mạo nơi quý vị sẽ được khuyến khích đăng nhập vào tài khoản hoặc nhập các chi tiết bí mật.

Các cuộc tấn công lừa đảo thường xâm phạm mật mã tài khoản của quý vị. Tội phạm mạng thường sử dụng phương pháp này để "chiếm lấy" các tài khoản mạng xã hội của các doanh nghiệp nhỏ và đòi tiền chuộc.

Cách thức để giảm thiểu

Nếu thông điệp đến từ một nơi quen biết nhưng có vẻ đáng nghi ngờ, hãy thận trọng. Hãy liên lạc riêng với người hoặc doanh nghiệp đó để kiểm tra xem tin nhắn có đúng không. Sử dụng các chi tiết liên lạc mà quý vị tìm thấy qua một nguồn hợp pháp, chẳng hạn như bằng cách truy cập trang mạng chính thức của doanh nghiệp đó, chứ không phải qua những chi tiết đáng nghi ngờ được viết trong thông điệp.

Hãy tìm hiểu thêm về cách để xác định các hành vi lừa đảo và tấn công lừa đảo qua các nguồn lực sau đây:

- Nhận biết và trình báo lừa đảo
- Tìm hiểu cách phát hiện các hành vi lừa đảo qua mạng
- Phát hiện các Thông điệp được Thiết kế Lợi dụng các Yếu tố Tâm lý để đánh lừa.

Nghiên cứu trường hợp:

Một nhân viên tại một công ty chuyển giao nhanh nhận được email từ một trong những nhân viên điều hành của họ, yêu cầu cô mua 6 thẻ tín dụng trả trước MasterCard mỗi thẻ trị giá 500 đô la. Giám đốc điều hành yêu cầu cô ấy giữ bí mật vì những tấm thẻ sẽ là phiếu quà tặng cho các nhân viên. Sau khi mua xong, cô nhân viên được yêu cầu chụp ảnh cả hai mặt của thẻ và gửi cho Nhân viên Điều hành để làm bằng chứng mua hàng.

Theo hướng dẫn, nhân viên đã đến một bưu điện và sử dụng thẻ tín dụng cá nhân của mình để mua thẻ quà tặng. Cô ấy trả lời email của giám đốc điều hành và gửi ảnh chụp các thẻ quà tặng để làm bằng chứng.

Sau khi từ bưu điện về, cô nhân viên đưa những tấm thẻ đó cho nhân viên điều hành – người không hề hay biết gì về chúng cả. Khi xem xét lại, **tất cả email về thẻ quà tặng đều đến từ một địa chỉ email ngẫu nhiên và không phải từ tài khoản email chính thức của người điều hành. Một trò lừa đảo vừa xảy ra.**

Các cuộc tấn công qua email

Ngoài các trò gian lận như lừa đảo trực tuyến, một cuộc tấn công email thường gặp nhằm vào các doanh nghiệp nhỏ là **xâm phạm email doanh nghiệp** (BEC). Tội phạm có thể mạo danh người đại diện doanh nghiệp bằng cách sử dụng tài khoản email bị xâm phạm, hoặc qua các phương tiện khác – chẳng hạn như sử dụng tên địa chỉ trang mạng trông giống với một doanh nghiệp có thật. Ngoài việc đánh cắp thông tin, mục tiêu của các cuộc tấn công này thường là để lừa nạn nhân gửi tiền vào tài khoản ngân hàng của những kẻ lừa đảo.

Cách thức để giảm thiểu

Cách tốt nhất để đối đầu với các cuộc tấn công email là đào tạo và nâng cao nhận thức cho nhân viên của quý vị. Phải bảo đảm là nhân viên của quý vị biết luôn thận trọng với các email có nội dung sau đây:

- yêu cầu thanh toán, đặc biệt là phải khẩn cấp hoặc đã quá hạn
- thay đổi chi tiết ngân hàng
- một địa chỉ email trông không ổn, chẳng hạn như tên địa chỉ trang mạng không ăn khớp chính xác với tên công ty của nhà cung cấp.

Mặc dù các cuộc tấn công này có thể gây nhiều tai hại, nhưng các biện pháp giảm thiểu thì dễ dàng và hầu như không tốn kém gì. **Khi nhân viên nhận được những email như thế này, cách giảm thiểu hiệu quả nhất là gọi điện thoại đến người gửi để xác nhận rằng những email này là xác thực.** Không sử dụng các chi tiết liên lạc mà quý vị đã nhận được vì đó có thể là giả mạo. Áp dụng một quy trình chính thức để nhân viên tuân theo khi nhận được yêu cầu thanh toán hoặc chi tiết ngân hàng được thay đổi.

Tìm hiểu cách bảo vệ doanh nghiệp của quý vị khỏi lừa đảo BEC và xâm phạm email qua các nguồn lực sau đây:

- Xâm phạm email doanh nghiệp
- Bảo vệ doanh nghiệp của quý vị từ các email gian lận và bị xâm phạm
- Cần phải làm gì nếu doanh nghiệp của quý vị là mục tiêu của hành vi gian lận email hoặc qua email bị xâm phạm.

Nghiên cứu trường hợp:

Một doanh nghiệp xây dựng nhỏ nhận được email từ nhà cung cấp cho biết họ đã thay đổi ngân hàng. Nhà cung cấp đã gửi các chi tiết tài khoản mới để thanh toán hóa đơn. Vì email trông có vẻ hợp pháp, **nên doanh nghiệp xây dựng đã không gọi cho nhà cung cấp để xác nhận việc thay đổi các chi tiết tài khoản ngân hàng.**

Doanh nghiệp đã thanh toán hơn 70,000 đô-la cho một hóa đơn từ nhà cung cấp này. Ngày hôm sau, một nhân viên khác lại thanh toán nhầm hóa đơn tương tự với số tiền bổ sung hơn 70,000 đô la. Tổng cộng, hơn 150,000 đô la đã được trả vào tài khoản ngân hàng mới.

Khi doanh nghiệp gọi điện cho nhà cung cấp của họ để hỏi liệu họ có thể hoàn trả khoản thanh toán trùng lặp hay không, nhà cung cấp đã thông báo rằng các chi tiết ngân hàng đó là không đúng. Một cuộc điều tra đã được tiến hành ngay lập tức, và nhà cung cấp phát hiện ra rằng một trong những tài khoản email của họ đã bị xâm phạm và đang gửi đi các thông tin tài khoản ngân hàng giả mạo. **Không có khoản tiền nào được thu hồi.**

Phần mềm độc hại

Phần mềm độc hại là thuật ngữ chung nói về các phần mềm độc hại được thiết kế để gây hại, chẳng hạn như phần mềm tống tiền, vi rút, phần mềm gián điệp và trojans (là một phiên bản giả mạo của ứng dụng). Phần mềm độc hại có thể:

- ăn cắp hoặc khóa các tập hồ sơ trên thiết bị của quý vị
- ăn cắp số thẻ ngân hàng hoặc thẻ tín dụng của quý vị
- ăn cắp tên đăng nhập và mật mã của quý vị
- kiểm soát hoặc thu thập thông tin trên máy tính của quý vị.

Phần mềm độc hại có thể ngăn chặn thiết bị của quý vị hoạt động bình thường, xóa hoặc làm hỏng các tập hồ sơ, hoặc cho phép người khác truy cập thông tin của cá nhân hoặc doanh nghiệp của quý vị. Nếu thiết bị của quý vị bị nhiễm phần mềm độc hại, quý vị có thể dễ trở thành mục tiêu cho các cuộc tấn công khác. Phần mềm độc hại cũng có thể lây lan sang các thiết bị khác trong mạng của quý vị

Thiết bị của quý vị có thể bị nhiễm phần mềm độc hại theo một số cách, bao gồm:

- truy cập các trang mạng đã bị nhiễm phần mềm độc hại
- tải xuống các tập hồ sơ hoặc phần mềm bị nhiễm từ internet
- mở tập hồ sơ đính kèm email bị nhiễm.

Phần mềm tống tiền

Phần mềm tống tiền là một loại độc hại thường gặp và nguy hiểm. Nó hoạt động bằng cách khóa hoặc mã hóa các tập hồ sơ của quý vị để quý vị không thể truy cập chúng được nữa. Một khoản tiền chuộc, thường là ở dạng tiền điện tử, được yêu cầu để khôi phục quyền truy cập vào các tập hồ sơ. Tội phạm mạng cũng có thể đe dọa đăng tải hoặc bán dữ liệu trực tuyến, trừ khi quý vị trả tiền chuộc.

Cách thức để giảm thiểu

Mặc dù phần mềm chống vi-rút hoặc phần mềm bảo mật có thể giúp bảo vệ quý vị khỏi phần mềm độc hại, nhưng không có phần mềm nào hiệu quả 100%. Nhân viên phải thận trọng với email, các trang mạng và các tập hồ sơ tải xuống, đồng thời phải thường xuyên cập nhật thiết bị của họ để giữ an toàn.

Xem các nguồn lực sau đây để biết thêm thông tin về cách bảo vệ doanh nghiệp của quý vị khỏi phần mềm tống tiền:

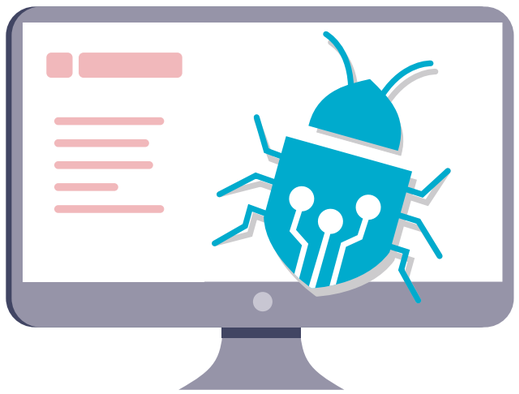
- Phần mềm tống tiền
- Tự bảo vệ mình trước các cuộc tấn công của mã độc tống tiền
- Cần phải làm gì nếu quý vị bị đòi tiền chuộc.

Nghiên cứu trường hợp:

Nhân viên của một cửa hàng phụ tùng ô tô đến sở làm vào một buổi sáng và không thể khởi động máy chủ của họ. Khi nhà cung cấp Công nghệ Thông tin của họ truy cập vào máy chủ, họ thấy một cửa sổ mở ra cho biết tất cả dữ liệu máy tính đã bị mã hóa. Có ghi chú yêu cầu họ trả tiền chuộc bằng bitcoin để mở khóa các tập hồ sơ.

Có một ổ đĩa sao lưu được cắm vào máy tính, ổ đĩa này cũng đã bị mã hóa. Họ đã cố gắng kết nối nhiều ổ đĩa dự phòng hơn, nhưng các tập hồ sơ đều bị mã hóa tự động trong vòng vài giây. **Họ đã không thể loại bỏ phần mềm tống tiền trước khi cố khôi phục dữ liệu của mình và làm mất tất cả các tập hồ sơ sao lưu mà họ có.**

Một cách duy nhất còn lại là khôi phục cài đặt gốc cho máy chủ và bắt đầu lại từ đầu bằng một hệ thống mới. Doanh nghiệp của họ bị mất dữ liệu lưu trữ của nhiều năm và phải bắt đầu lại từ đầu.



Bảo mật các tài khoản của quý vị

Bật tính năng xác thực đa yếu tố

Xác thực đa yếu tố (MFA) khiến tội phạm mạng khó truy cập vào tài khoản của quý vị hơn.

MFA đặt thêm một lớp phòng thủ khác vào tài khoản của quý vị. Đây là một trong những cách hiệu quả nhất để bảo vệ tài khoản của quý vị khỏi bị ai đó truy cập, vì vậy quý vị nên sử dụng nó trong mọi trường hợp có thể. Bất kỳ ai đăng nhập vào tài khoản của quý vị sẽ cần phải cung cấp thông thêm thông tin khác ngoài tên đăng nhập và mật mã. Đây có thể là một mã duy nhất từ tin nhắn hoặc qua một ứng dụng xác thực. Để biết thêm thông tin, hãy đọc lời khuyên của chúng tôi về MFA, có tại **cyber.gov.au/mfa**.

✓ **Bật MFA trong mọi trường hợp có thể, bắt đầu với các tài khoản quan trọng nhất của quý vị.**

Áp dụng biện pháp kiểm soát truy cập

Hạn chế quyền truy cập của người dùng có thể hạn chế thiệt hại do các vấn đề ninh mạng gây ra.

Kiểm soát truy cập là một cách để giới hạn quyền truy cập vào một số tập hồ sơ và hệ thống. Thông thường, nhân viên không cần quyền truy cập đầy đủ vào tất cả dữ liệu, tài khoản, và hệ thống trong doanh nghiệp. Họ chỉ nên được phép truy cập những gì họ cần để thực hiện công việc của họ mà thôi.

Hạn chế quyền truy cập của người dùng có thể hạn chế thiệt hại do vấn đề an ninh mạng gây ra. Ví dụ: nếu máy tính của một nhân viên bị nhiễm mã độc tống tiền, thì với các biện pháp kiểm soát truy cập thích hợp, mã độc đó chỉ có thể ảnh hưởng đến một số lượng nhỏ các tập hồ sơ chứ không đến toàn bộ doanh nghiệp.

✓ **Phải bảo đảm rằng mỗi người dùng chỉ có thể truy cập những gì họ cần cho vai trò của họ mà thôi.**

Sử dụng mật mã mạnh hoặc cụm mật mã

Bảo vệ tài khoản của quý vị khỏi tội phạm mạng bằng mật mã hoặc cụm mật mã an toàn.

Nhiều doanh nghiệp nhỏ phải đối mặt với các cuộc tấn công mạng do cách thức sử dụng mật mã kém.

Ví dụ: sử dụng lại cùng một mật mã trên nhiều tài khoản. Quý vị có thể sử dụng cả lập trình quản lý mật mã và cụm mật mã để tạo mật mã mạnh.

Lập trình quản lý mật mã giống như một 'két sắt' để cất giữ mật mã của quý vị. Quý vị có thể sử dụng nó để tạo và lưu trữ mật mã mạnh, **duy nhất** cho từng tài khoản của mình. Nếu quý vị có nhiều tài khoản, việc này sẽ giúp quý vị không phải nhớ nhiều mật mã. Quý vị không cần phải nhớ mật mã hoặc tài khoản có mật mã đó, vì tất cả đều được ghi lại trong lập trình quản lý mật mã của mình.

Đối với các tài khoản mà quý vị đăng nhập thường xuyên, hoặc nếu quý vị không muốn lưu trữ trong lập trình quản lý mật mã, hãy cân nhắc sử dụng cụm mật mã để làm mật mã cho mình. Cụm mật mã là sự kết hợp của các từ ngẫu nhiên, ví dụ: 'bánh quy đất sét hành tây pha lê'. Cụm mật mã rất hữu ích khi quý vị muốn có một mật mã an toàn, và dễ nhớ. Sử dụng kết hợp ngẫu nhiên bốn từ trở lên và giữ cho mật mã đó luôn là độc nhất – **không sử dụng lại cụm mật mã** trên nhiều tài khoản. Để biết thêm thông tin, hãy đọc lời khuyên của chúng tôi về cụm mật mã và lập trình quản lý mật mã , có tại **cyber.gov.au/passphrases**.

✓ **Sử dụng lập trình quản lý mật mã để tạo và lưu trữ các mật mã duy nhất cho từng tài khoản quan trọng của quý vị.**

Quản lý các tài khoản dùng chung

Các tài khoản được sử dụng chung có thể ảnh hưởng đến việc bảo mật và gây khó khăn cho việc theo dõi các hoạt động độc hại.

Trong một doanh nghiệp nhỏ, có thể có những lý do chính đáng khiến nhân viên cần chia sẻ tài khoản, nhưng nên tránh càng nhiều càng tốt. Khi nhiều nhân viên sử dụng chung một tài khoản, điều này có thể khó để theo dõi hoạt động của từng người, và lại càng khó hơn để theo dõi tội phạm mạng xâm nhập. Trừ khi quý vị thay đổi mật mã, các nhân viên cũ cũng có thể tiếp tục truy cập tài khoản ngay cả khi họ đã rời khỏi doanh nghiệp.

✓ **Hạn chế sử dụng các tài khoản được dùng chung và bảo mật bất kỳ tài khoản nào được sử dụng trong doanh nghiệp của quý vị.**

Bảo vệ thiết bị và thông tin của quý vị

Cập nhật phần mềm của quý vị

Luôn cập nhật phần mềm của quý vị là một trong những cách tốt nhất để bảo vệ doanh nghiệp của quý vị khỏi một cuộc tấn công mạng.

Các bản cập nhật có thể khắc phục các lỗi bảo mật trong hệ điều hành và phần mềm khác của quý vị, do đó tội phạm mạng khó đột nhập hơn. Các lỗ hổng mới luôn được phát hiện, vì vậy đừng bỏ qua các lời nhắc nhở cập nhật. Thường xuyên cập nhật phần mềm của quý vị sẽ làm giảm cơ hội tội phạm mạng sử dụng các điểm yếu đã được biết để chạy phần mềm độc hại hoặc đột nhập vào thiết bị của quý vị. Nếu quý vị cần trợ giúp, ACSC đã xuất bản hướng dẫn về các bản cập nhật.

Nếu thiết bị hoặc phần mềm của quý vị quá cũ thì có thể không có bản cập nhật. Nếu nhà sản xuất đã ngừng hỗ trợ cho sản phẩm bằng các bản cập nhật, quý vị nên cân nhắc nâng cấp lên một sản phẩm mới hơn để duy trì sự an toàn. Ví dụ về các hệ thống điều hành không còn nhận được các bản cập nhật quan trọng là **iPhone 7** và **Microsoft Windows 7**.

Để biết thêm thông tin, hãy đọc hướng dẫn cập nhật của chúng tôi, có trên **cyber.gov.au/updates**.

✓ **Bật cập nhật tự động cho thiết bị và phần mềm của quý vị.**

Sử dụng phần mềm bảo mật

Phần mềm bảo mật như chống vi-rút và chống mã độc tống tiền có thể giúp bảo vệ thiết bị của quý vị.

Sử dụng phần mềm bảo mật để phát hiện và loại bỏ phần mềm độc hại khỏi thiết bị của quý vị. Phần mềm chống vi-rút có thể được cài đặt để thường xuyên quét các tập hồ sơ và các chương trình khả nghi. Khi phát hiện thấy mối đe dọa, quý vị sẽ nhận được cảnh báo và các tập hồ sơ đáng ngờ sẽ được kiểm tra hoặc loại bỏ.

Nhiều doanh nghiệp nhỏ có thể **sử dụng lập trình Bảo mật của Windows** để tự bảo vệ mình khỏi vi-rút và phần mềm độc hại. Bảo mật của Windows được tích hợp sẵn cho các thiết bị Windows 10 và Windows 11, đồng thời bao gồm chức năng bảo vệ miễn phí khỏi các mối đe dọa và vi-rút. Quý vị cũng có thể sử dụng nó để bật các tính năng bảo vệ khỏi phần mềm tống tiền trên thiết bị của mình.

Để biết các tùy chọn và sản phẩm thay thế, hãy đọc lời khuyên của chúng tôi về phần mềm diệt vi-rút bằng cách tìm kiếm *phần mềm chống vi-rút* trên cyber.gov.au.

✓ **Thiết lập phần mềm bảo mật để hoàn tất quá trình quét thường xuyên trên thiết bị của quý vị.**

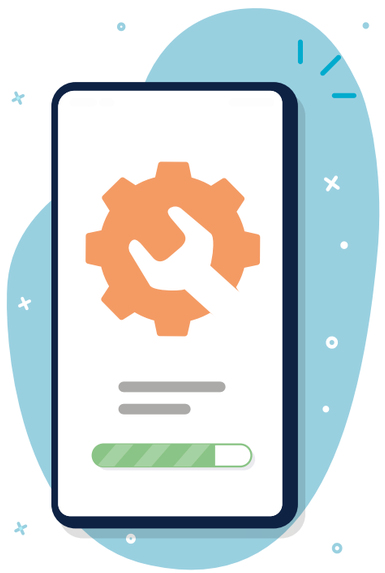
Sao lưu thông tin của quý vị

Sao lưu thường xuyên có thể giúp quý vị khôi phục thông tin của mình nếu thông tin đó bị mất hoặc bị xâm phạm.

Quý vị nên thường xuyên sao lưu hoặc cài đặt để máy tự động sao lưu hồ sơ doanh nghiệp của mình. Nếu không có bản sao lưu thường xuyên, quý vị có thể sẽ rất khó để khôi phục thông tin của mình sau một cuộc tấn công mạng.

Có nhiều cách và sản phẩm để giúp cho quý vị sao lưu thông tin của mình. Để được hướng dẫn cặn kẽ về cách thức sao lưu cho doanh nghiệp của quý vị, hãy đọc lời khuyên về sao lưu của chúng tôi, có sẵn tại **cyber.gov.au/backups**. Phương pháp tốt nhất sẽ còn tuỳ thuộc vào từng doanh nghiệp, vì vậy hãy nói chuyện với chuyên gia Công nghệ Thông tin nếu quý vị không chắc chắn.

✓ **Hãy tạo lập một kế hoạch và thực hiện để thường xuyên sao lưu thông tin của mình.**



Bảo mật mạng của quý vị và các dịch vụ bên ngoài

Bảo vệ doanh nghiệp của quý vị khỏi một cuộc tấn công mạng bằng cách giải quyết các lỗ hổng tiềm ẩn trong mạng của mình.

Các thiết bị và dịch vụ sử dụng mạng của quý vị có thể là mục tiêu chính của tội phạm mạng. Nhiều trong số các hệ thống này có thể phức tạp để bảo mật, vì vậy hãy thảo luận các đề nghị sau đây với chuyên gia Công nghệ Thông tin.

- **Bảo mật máy chủ của quý vị** : Nếu bạn sử dụng NAS hoặc máy chủ khác trong nhà hoặc doanh nghiệp của mình, hãy cẩn thận hơn để bảo mật chúng. Các thiết bị này là mục tiêu thường gặp đối với tội phạm mạng, vì chúng thường lưu trữ các tập hồ sơ quan trọng hoặc để thực hiện các chức năng thiết yếu. Có nhiều phương pháp giảm thiểu cần thiết để bảo vệ các thiết bị này. Ví dụ: điều quan trọng là phải bảo đảm tất cả các máy chủ hoặc thiết bị NAS được cập nhật thường xuyên. Tài khoản quản trị nên được bảo mật bằng cụm mật mã mạnh hoặc bằng tính năng xác thực đa yếu tố.

- **Giảm thiểu các dấu chân 'điện tử' bên ngoài**: Kiểm tra và bảo mật mọi dịch vụ trên mạng của quý vị mà có truy cập internet. Điều này có thể bao gồm Máy vi tính Từ xa, các tập Hồ sơ được Chia sẻ, Điện thư và các dịch vụ quản trị từ xa.

- **Chuyển sang dịch vụ 'đám mây':** Hãy xem xét đến việc sử dụng các dịch vụ trực tuyến hoặc đám mây có sẵn tính năng bảo mật tích hợp, thay vì tự quản lý. Ví dụ: sử dụng các dịch vụ trực tuyến cho những thứ như email hoặc lưu trữ trang mạng thay vì tự điều khiển và bảo mật các dịch vụ này.

- **Cải thiện bảo mật cho thiết bị định tuyến của quý vị:** Làm theo hướng dẫn của chúng tôi về các cách bảo mật thiết bị định tuyến của quý vị, bao gồm cập nhật mật mã mặc định, bật Wi-Fi "Khách" cho khách hàng hoặc khách truy cập, và sử dụng các giao thức mã hóa mạnh nhất. Tìm kiếm *thiết định tuyến* trên **cyber.gov.au** để biết thêm thông tin.

- **Tìm hiểu về chuỗi cung ứng mạng của quý vị:** Các doanh nghiệp hiện đại thường thuê mướn nhiều dịch vụ bên ngoài. Ví dụ: sử dụng Nhà cung cấp Dịch vụ được Quản lý để bảo trì bộ phận Công nghệ Thông tin của họ. Các vấn đề bảo mật với các dịch vụ hoặc nhà cung cấp này có thể có tác động đáng kể đến doanh nghiệp của quý vị. Để biết hướng dẫn cặn kẽ về việc quản lý rủi ro cho các chuỗi cung ứng trên mạng, hãy đọc Hướng dẫn về Chuỗi Cung ứng trên Mạng của chúng tôi trên **cyber.gov.au**.

✓ **Trao đổi với chuyên gia Công nghệ Thông tin về các cách bảo mật mạng của quý vị.**

Tăng cường phòng thủ cho trang mạng của quý vị

Các trang mạng là mục tiêu chính cho các cuộc tấn công mạng.

Bảo vệ trang mạng của quý vị khỏi bị tấn công bằng cách làm theo một số biện pháp bảo mật cơ bản:

- bảo mật thông tin đăng nhập trang mạng của quý vị bằng xác thực đa yếu tố hoặc mật mã mạnh
- thường xuyên cập nhật các phần bổ sung và hệ thống quản lý nội dung trang mạng của quý vị
- sao lưu trang mạng của mình thường xuyên để quý vị có thể khôi phục nó sau một cuộc tấn công mạng.

ACSC có sẵn các nguồn lực bổ sung dành cho chủ sở hữu trang mạng. Tìm kiếm các nguồn lực này trên **cyber.gov.au**:

- Những Sửa đổi Đơn giản Nhanh chóng và Dễ dàng Thực hiện cho Trang mạng của quý vị (Quick Wins)
- Áp dụng Chứng chỉ, TLS, HTTPS và Opportunistic TLS (cho phép các máy chủ nhận chuyển thư được mã hóa để bảo vệ email)
- Hệ thống Bảo mật Địa chỉ Trang mạng cho Chủ Sở hữu Địa chỉ Trang mạng
- Chuẩn bị và Đối phó với các Cuộc Tấn công nhằm Tắt Máy hoặc Mạng (Denial-of-Service Attacks)

✓ **Đọc qua các nguồn lực của ACSC về bảo mật trang mạng.**

Khôi phục cài đặt gốc các thiết bị của quý vị trước khi bán hoặc bỏ đi

Dữ liệu trên các thiết bị cũ của quý vị có thể bị người khác truy cập.

Nếu quý vị không vứt bỏ thiết bị của mình một cách an toàn, tội phạm mạng có thể truy cập thông tin trên các thiết bị đó. Các thông tin này có thể bao gồm email, tập hồ sơ và các dữ liệu kinh doanh khác. Xóa hết tất cả thông tin khỏi thiết bị kinh doanh của mình trước khi bán, trao đổi hoặc vất bỏ chúng. Ví dụ: bằng cách thực hiện khôi phục cài đặt gốc. Việc này sẽ giúp xóa tất cả các thông tin và khôi phục thiết bị về cài đặt gốc.

Để biết hướng dẫn về cách đặt lại thiết bị của quý vị, hãy đọc hướng dẫn của chúng tôi về cách thức vứt bỏ thiết bị của mình một cách an toàn. Tìm kiếm *vất bỏ đi* trên trang **cyber.gov.au**.

✓ **Thực hiện khôi phục cài đặt gốc trước khi bán hoặc vất bỏ đi các thiết bị kinh doanh.**

Khoá và giữ cho thiết bị của quý vị an toàn

Hạn chế quyền truy cập vào các thiết bị kinh doanh của quý vị sẽ làm giảm cơ hội cho các hoạt động độc hại.

Hạn chế quyền truy cập sử dụng các thiết bị kinh doanh của quý vị là một cách đơn giản để ngăn ngừa dữ liệu bị đánh cắp hoặc ngăn ngừa các hoạt động độc hại khác. Không nên cất giữ các thiết bị của doanh nghiệp ở một nơi mà các nhân viên, hoặc công chúng không không phận sự có thể sử dụng và truy cập được.

Sử dụng các biện pháp kiểm soát bảo mật để tăng cường phòng thủ cho các thiết bị doanh nghiệp của quý vị. Ở mức tối thiểu, thiết bị phải được khóa bằng cụm mật mã, mã PIN hoặc sinh trắc học (vân tay, nhận dạng, mống mắt v.v...). Phải bảo đảm các thiết bị này được cài đặt để tự động khóa sau một thời gian ngắn không hoạt động.

✓ **Định cấu hình thiết bị để tự động khóa sau một thời gian ngắn không hoạt động.**

Bảo vệ dữ liệu kinh doanh của quý vị

Dữ liệu do doanh nghiệp của quý vị nắm giữ là mục tiêu hấp dẫn đối với tội phạm mạng.

Các vụ xâm phạm dữ liệu ngày càng gia tăng – đừng để doanh nghiệp của mình trở thành nạn nhân. Điều quan trọng là phải hiểu doanh nghiệp của quý vị nắm giữ dữ liệu gì và nằm ở đâu. Khi quý vị đã biết, hãy sử dụng các phương cách trong hướng dẫn này để giúp bảo vệ dữ liệu của quý vị khỏi việc bị tội phạm mạng truy cập. Một số doanh nghiệp nhỏ cũng có thể có các bổn phận thêm theo luật pháp.

- **Nhập chung dữ liệu doanh nghiệp của quý vị.** Quý vị có thể có dữ liệu được lưu trữ trên nhiều thiết bị hoặc dịch vụ. Khi dữ liệu được phân cấp, số lượng hệ thống quý vị phải bảo mật và sao lưu sẽ tăng lên. Khi có nhiều hệ thống, điều này cũng có thể tạo ra nhiều cơ hội hơn để tội phạm mạng tấn công. Những khi có thể, hãy lưu trữ dữ liệu kinh doanh của quý vị ở một địa điểm trung tâm an toàn và được sao lưu thường xuyên. Việc tập trung hóa dữ liệu của quý vị có thể tạo ra lỗ hổng lớn hơn nếu hệ thống của bạn bị xâm phạm, vì vậy hãy chắc chắn rằng vị trí trung tâm này tâm được bảo vệ đầy đủ bằng các cấu hình an toàn và hạn chế quyền truy cập. Nói chuyện với chuyên gia Công nghệ Thông tin hoặc chuyên viên về an ninh mạng để được cố vấn.
- **Hiểu biết về các bổn phận của mình về bảo vệ dữ liệu.** Một số doanh nghiệp nhỏ có thể có các bổn phận pháp lý để kiểm soát các thông tin cá nhân mà họ thu thập. Đọc hướng dẫn của Ủy viên Văn phòng Thông tin Úc dành cho các doanh nghiệp nhỏ để tìm hiểu thêm, có sẵn tại **oaic.gov.au**. Tham khảo với chuyên gia về pháp lý nếu quý vị không chắc chắn.

✓ **Hiểu về các trách nhiệm của mình trong việc bảo vệ các dữ liệu doanh nghiệp mà quý vị nắm giữ.**

Trang bị cho nhân viên của quý vị

Hướng dẫn cho nhân viên

Nhân viên có các thông lệ tốt về an ninh mạng, là tuyến phòng thủ đầu tiên của quý vị trước các cuộc tấn công mạng.

Nhân viên của quý vị nên có nhận thức về vấn đề an ninh mạng, bao gồm các chủ đề sau:

- các mối đe dọa an ninh mạng thường gặp như email doanh nghiệp bị xâm phạm và mã độc tống tiền
- các biện pháp bảo vệ bao gồm mật mã hoặc cụm mật mã mạnh, xác thực đa yếu tố (MFA) và cập nhật phần mềm
- cách phát hiện lừa đảo và tấn công lừa đảo
- các chính sách đặc thù của riêng doanh nghiệp (ví dụ: quy trình để trình báo email đáng ngờ hoặc để xác thực hóa đơn trước khi thanh toán)
- cần phải làm gì trong trường hợp khẩn cấp.

Trang mạng của ACSC có các nguồn lực cho hầu hết các chủ đề này tại địa chỉ cyber.gov.au/learn. Quý vị có thể xem xét các cách thức khác để huấn luyện nhân viên của mình, chẳng hạn như bằng một khóa học chính thức hoặc đào tạo nội bộ. Dù quý vị quyết định thế nào, hãy nhớ rằng việc huấn luyện cho nhân viên về vấn đề an ninh mạng không phải là việc chỉ có một lần, mà phải được cập nhật định kỳ.

✓ **Xác định phương cách huấn luyện về nhận thức an ninh mạng trong doanh nghiệp của quý vị.**

Tạo lập kế hoạch khẩn cấp

Có một kế hoạch khẩn cấp có thể làm giảm tác động của một cuộc tấn công mạng đối với doanh nghiệp của quý vị.

Khi phải đối phó với vấn đề an ninh mạng, quý vị không có nhiều thời gian. Có một kế hoạch khẩn cấp nghĩa là nhân viên của quý vị sẽ không phí thời gian để tìm ra những việc cần phải làm, mà họ sẽ biết phải làm gì.

Hãy xem xét đến các câu hỏi sau đây khi tạo lập kế hoạch khẩn cấp:

- Quy trình để nhân viên của quý vị trình báo các vấn đề an ninh mạng tiềm ẩn là gì?
- Quý vị phải liên lạc với ai để được hỗ trợ? Ví dụ như các chuyên gia Công nghệ Thông tin và ngân hàng của quý vị.
- Sự việc sẽ được thông báo bằng cách nào tới nhân viên, các bên liên quan, hoặc khách hàng của quý vị?
- Quý vị phải làm sao để giữ cơ sở kinh doanh của mình hoạt động như bình thường, nếu bất kỳ hệ thống quan trọng nào đang bị ngoại tuyến?

Phải chắc chắn rằng nhân viên của quý vị đã quen thuộc với kế hoạch khẩn cấp, bao gồm mọi vai trò hoặc trách nhiệm mà họ có thể có. Phải có một bản sao bằng giấy của kế hoạch này phòng khi hệ thống của quý vị bị ngoại tuyến.

✓ **Tạo lập một kế hoạch khẩn cấp cho các vấn đề an ninh mạng.**

Luôn cập nhật thông tin

Trở thành đối tác của ACSC để nhận những thông tin mới nhất từ ACSC.

Cập nhật thông tin về các mối đe dọa và lỗ hổng mạng mới nhất bằng cách trở thành đối tác của ACSC. Dịch vụ này sẽ gửi cho quý vị các bản tin hàng tháng và cảnh báo khi một mối đe dọa mạng mới được xác định.

An ninh mạng là một lĩnh vực phát triển nhanh chóng. Tội phạm mạng sẽ tích cực khai thác các lỗ hổng chỉ trong vòng vài phút sau khi phát hiện ra chúng. Cập nhật thông tin về bối cảnh an ninh mạng sẽ giúp cho doanh nghiệp của quý vị hiểu được các mối đe dọa mà doanh nghiệp có thể gặp phải và các phương cách để đối phó.

✓ **Đăng ký doanh nghiệp của quý vị với Chương trình Đối tác ACSC.**

Tuyên bố miễn trừ trách nhiệm

Tài liệu trong hướng dẫn này mang tính chất tổng quát và không nên được coi là tư vấn pháp lý, hoặc được dựa vào để được hỗ trợ trong bất kỳ trường hợp cụ thể hoặc tình huống khẩn cấp nào. Đối với bất kỳ vấn đề quan trọng nào, quý vị nên tìm kiếm lời khuyên chuyên môn, độc lập, và thích hợp liên quan đến các hoàn cảnh của mình.

Chính phủ Liên bang không chịu trách nhiệm hoặc trách nhiệm pháp lý nào đối với bất kỳ thiệt hại, mất mát hoặc chi phí nào phát sinh do việc trông cậy vào thông tin có trong hướng dẫn này.

Muốn biết thêm thông tin, hoặc muốn trình báo vấn đề an ninh mạng, hãy liên lạc với chúng tôi:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Số điện thoại này chỉ được sử dụng ở trong nước Úc mà thôi.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre