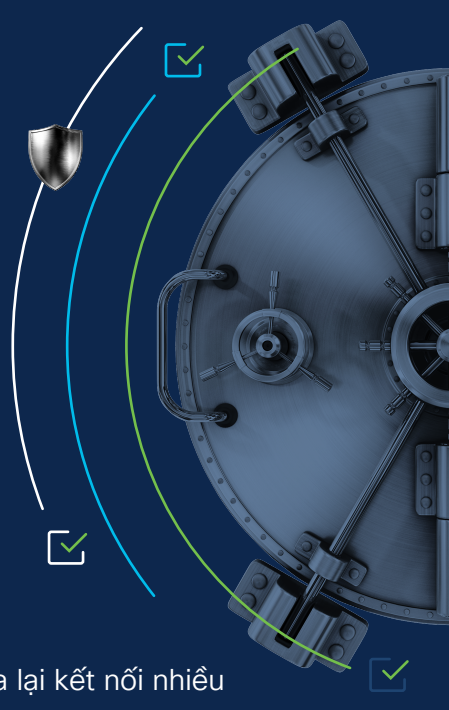
CISCO
SECURE

5 cách thiết thực để củng cố an ninh mạng



Những thách thức về an ninh mạng sẽ luôn tồn tại. Mỗi ngày, thế giới của chúng ta lại kết nối nhiều hơn và phức tạp hơn. Đối với các đội ngũ an ninh mạng, mức độ phức tạp cao hơn đồng nghĩa với trách nhiệm nhiều hơn.

May mắn thay, các công ty có thể thực hiện các biện pháp cụ thể để cải thiện kết quả bảo mật. Trong Nghiên cứu kết quả bảo mật, tập 2, chúng tôi đã thu thập dữ liệu từ hơn 5.100 chuyên gia bảo mật và CNTT trên 27 quốc gia. Từ dữ liệu đó, chúng tôi đã tập trung vào năm phương thức chính đã được kiểm chứng về khả năng thúc đẩy thành công của chương trình an ninh mạng. Hãy tận dụng danh sách dưới đây:

Làm mới công nghệ

39% công nghệ bảo mật mà các tổ chức sử dụng bị coi là công nghệ lỗi thời.

Đừng vội phản ứng, hãy đánh giá nền tảng công nghệ của bạn sau một sự cố xem. Hãy xây dựng chiến lược chủ động làm mới công nghệ ngay hôm nay!

> “Với gần 40% các tổ chức sử dụng công nghệ bảo mật lạc hậu, gánh nặng bảo mật là vấn đề gây đau đầu. Nhưng tin mừng là các tổ chức có kiến trúc đám mây hợp nhất hiện đại đạt được mức độ làm mới công nghệ cao bằng cách chủ động trong chiến lược công nghệ của họ. Vỏ quýt dày có móng tay nhọn.”
>
> Richard Archdeacon, Giám đốc tư vấn an toàn thông tin, Cisco

Tích hợp để có khả năng hiển thị tốt hơn

77% tổ chức muốn mua các giải pháp tích hợp hơn là tự xây dựng.

May mắn thay, các giải pháp dựa trên đám mây ngày càng trở nên nổi bật, các phần tích hợp mạnh mẽ dễ tiếp cận hơn bao giờ hết, nhờ vậy mà các đội ngũ bảo mật có được khả năng hiển thị rộng hơn trên hệ thống.

> “CNTT bảo mật hiện đại và tích hợp tốt là yếu tố góp phần vào thành công chung của chương trình, hiệu quả hơn bất kỳ phương thức bảo mật hoặc kiểm soát nào khác.”
>
> Helen Patton, Giám đốc tư vấn an toàn thông tin, Cisco

Mở rộng đội ngũ

Các tổ chức có tỷ lệ nhân sự cao nhất có khả năng phát hiện và ứng phó với mối đe dọa cao hơn 20%.

Không thể mở rộng đội ngũ ư? Hãy xem xét việc củng cố các kỹ năng và sự thành thạo của nhân sự hiện có. Đào tạo luôn là một khoản đầu tư thông minh.

> “Hãy chọn ra những người có chuyên môn cao nhất cho đội ngũ điều hành an toàn thông tin của bạn, chất lượng hơn số lượng. Tự động hóa có thể giúp bạn thu hẹp khoảng cách với nhân viên cấp thấp của mình để kết quả đạt được không chênh lệch so với nhân viên cấp cao.”
>
> Wendy Nather, Tổng giám đốc tư vấn an toàn thông tin, Cisco

Làm việc thông minh hơn với thông tin về mối đe dọa

Các tổ chức sử dụng thông tin về mối đe dọa có khả năng phát hiện và phản ứng mạnh mẽ gấp 2 lần.

Cho dù có thể phát triển đội ngũ hay không, hãy sử dụng mọi công cụ phân tích thông tin sẵn có để thu hẹp khoảng cách đó. Làm việc thông minh hơn để gặt hái kết quả tốt hơn.

> “Khi doanh nghiệp kết hợp con người, quy trình và công nghệ mạnh mẽ cùng với thông tin chắc chắn về mối đe dọa, họ sẽ có được khả năng tiên tiến trong việc phát hiện và ứng phó với các nguy cơ.”
>
> Dave Lewis, Giám đốc tư vấn an toàn thông tin, Cisco

Cố ý phá vỡ mọi thứ

Các công ty tham gia thử nghiệm kỹ thuật hỗn loạn có thể tăng gấp 2 lần khả năng đảm bảo tính liên tục trong kinh doanh.

Nếu sự gián đoạn CNTT xảy ra thường xuyên và có chủ đích, tổ chức của bạn sẽ được chuẩn bị để xử lý các mối đe dọa thực sự. Nắm bắt sự hỗn loạn để chuẩn bị cho sự hỗn loạn.

> “Các tổ chức thực hiện các thử nghiệm thường xuyên và đa dạng có khả năng duy trì hoạt động trong trường hợp khẩn cấp cao gấp 2,5 lần. Khả năng này có thể được củng cố hơn nữa khi tuân theo các phương pháp kỹ thuật hỗn loạn.”
>
> Wolfgang Goerlich, Giám đốc tư vấn an toàn thông tin, Cisco

Các bước này đều được chứng minh bằng dữ liệu, nếu làm theo, bạn sẽ cải thiện được hệ thống an ninh mạng. Nhưng đừng chỉ nghe theo lời chúng tôi. Để xem tất cả dữ liệu đằng sau nghiên cứu của chúng tôi, hãy xem báo cáo đầy đủ ngay hôm nay.

Xem báo cáo

CISCO The bridge to possible