1. Các yếu tố của chính sách nhận thức & đào tạo

1.1 Tổng quan

Đối với mỗi rủi ro và mối đe dọa đã xác định trong Miền Người Dùng và Miền Máy Trạm, hãy xác định một kiểm soát bảo mật hoặc biện pháp đối phó bảo mật có thể giúp giảm thiểu rủi ro hoặc mối đe dọa.

Domain	Rủi ro & Mối đe dọa	Chiến lược/Tài liệu Giảm thiểu Rủi ro
User Domain	Xử lý con người và bản chất con người	Đào tạo định kỳ; thực thi chính sách
	Sự thờ ơ của người dùng hoặc nhân viên đối với chính sách bảo mật hệ thống thông tin	Lọc Web
	Truy cập Internet giống như mở "hộp Pandora" do mối đe dọa từ kẻ tấn công	Các cổng an toàn
	Lướt web có thể là một hành trình nguy hiểm trong lãnh thổ chưa biết	Kiểm soát ứng dụng
	Mở e-mail và tệp đính kèm e-mail không xác định có thể giải phóng phần mềm và mã độc hại	Lọc mail
Workstation Domain	Cài đặt ứng dụng, tệp hoặc dữ liệu không được ủy quyền trên tài sản CNTT thuộc sở hữu của tổ chức có thể nguy hiểm	Giám sát
	Tải xuống ứng dụng hoặc phần mềm chứa phần mềm hoặc mã độc hại ẩn	Bảo mật điểm cuối
	Nhấp vào liên kết URL không xác định với các tập lệnh ẩn	Lọc URL

	Truy cập trái phép vào máy trạm	MFA; mật khẩu mạnh; khóa tự động
	Lỗ hổng phần mềm hệ điều hành	Quản lý vá lỗi
	Lỗ hổng phần mềm ứng dụng	Antivirus
	Virus, Trojan, sâu máy tính, phần mềm gián điệp, phần mềm/mã độc hại, v.v	Vô hiệu hóa cổng hoặc kiểm soát truy cập phương tiện
	Người dùng chèn đĩa CD, DVD, ổ USB chứa tệp cá nhân vào tài sản CNTT thuộc sở hữu của tổ chức	EDR
	Người dùng tải xuống ứng dụng và phần mềm không được ủy quyền vào tài sản CNTT thuộc sở hữu của tổ chức	Hạn chế quyền quản trị
	Người dùng cài đặt ứng dụng và phần mềm không được ủy quyền vào tài sản CNTT thuộc sở hữu của tổ chức	Giám sát cài đặt phần mềm

1.2 Các yếu tốt của chính sách nhận thức & đào tạo

1.2.1 Tổng quan

Trong bài thực hành này, bạn sẽ tạo một chính sách nhận thức & đào tạo bảo mật toàn tổ chức cho một tổ chức giả định để phản ánh các yêu cầu của một luật tuân thủ gần đây. Dưới đây là kịch bản của bạn:

• Ngân hàng tín dụng ABC khu vực với nhiều chi nhánh và địa điểm trên toàn khu vực

• Ngân hàng trực tuyến và sử dụng Internet là điểm mạnh của ngân hàng do nguồn nhân lực hạn chế

• Bộ phận dịch vụ khách hàng là chức năng/hoạt động kinh doanh quan trọng nhất của tổ chức

• Tổ chức muốn tuân thủ GLBA và các thực hành bảo mật CNTT tốt nhất liên quan đến nhân viên trong Miền Người Dùng và Miền Máy Trạm

• Tổ chức muốn giám sát và kiểm soát việc sử dụng Internet bằng cách triển khai lọc nội dung

• Tổ chức muốn loại bỏ việc sử dụng cá nhân tài sản và hệ thống CNTT thuộc sở hữu của tổ chức

• Tổ chức muốn giám sát và kiểm soát việc sử dụng hệ thống e-mail bằng cách triển khai các kiểm soát bảo mật e-mail

• Tổ chức muốn triển khai chính sách nhận thức & đào tạo bảo mật bắt buộc cho tất cả nhân viên mới và nhân viên hiện tại. Định nghĩa chính sách bao gồm yêu cầu GLBA và dữ liệu quyền riêng tư khách hàng và bắt buộc đào tạo nhận thức bảo mật hàng năm cho tất cả nhân viên

1.2.2 Hướng dẫn

Sử dụng Microsoft Word, tạo Chính sách Nhận thức & Đào tạo Bảo mật cho Ngân hàng Tín dụng ABC nắm bắt các yếu tố của chính sách như được định nghĩa trong Bảng Đánh giá Bài Thực hành #5 – Lab. Sử dụng mẫu chính sách sau để tạo định nghĩa Chính sách Nhận thức & Đào tạo Bảo mật của bạn.

- Chính sách

Chính sách Nhận thức & Đào tạo Bảo mật này nhằm thiết lập hướng dẫn và quy trình để bảo vệ dữ liệu, hệ thống và nhân sự của Ngân hàng Tín dụng ABC bằng cách đảm bảo rằng tất cả nhân viên, nhà thầu và nhân sự bên thứ ba hiểu và tuân thủ các thực hành bảo mật để giảm thiểu rủi ro.

- Mục đích

Mục đích của chính sách này là cung cấp một cách tiếp cận có cấu trúc đối với đào tạo bảo mật, tăng cường nhận thức về các mối đe dọa an ninh mạng và thúc đẩy các thực hành an toàn để giảm lỗ hổng bảo mật và đảm bảo tuân thủ quy định.

- Phạm vi

Chính sách này áp dụng cho tất cả nhân viên Ngân hàng Tín dụng ABC, nhà thầu và nhân sự bên thứ ba có quyền truy cập vào hệ thống thông tin, dữ liệu hoặc cơ sở vật chất của tổ chức.

- Tiêu chuẩn

Đào tạo Bắt buộc: Tất cả nhân viên mới phải hoàn thành đào tạo bảo mật trong vòng 30 ngày kể từ ngày nhận việc. Đào tạo ôn tập hàng năm là bắt buộc đối với tất cả nhân viên.

- Đào tạo Chuyên biệt: Đào tạo bảo mật bổ sung là bắt buộc đối với các vai trò có quyền truy cập hệ thống hoặc dữ liệu nâng cao.
- Mô phỏng Lừa đảo: Các mô phỏng lừa đảo hàng quý sẽ đánh giá nhận thức và phản ứng của nhân viên.

- Quy trình

- Triển khai Đào tạo: Đào tạo bảo mật sẽ được cung cấp trực tuyến hoặc trực tiếp và phải được hoàn thành trước các thời hạn được chỉ định.
- Theo dõi Tuân thủ: Tỷ lệ tham gia và hoàn thành sẽ được theo dõi bởi Nhân viên Bảo mật.
- Báo cáo Sự cố: Nhân viên được yêu cầu báo cáo bất kỳ sự cố bảo mật hoặc hoạt động đáng ngờ ngay lập tức cho Bảo mật CNTT.

- Hướng dẫn

- Duyệt Web An toàn: Nhân viên nên tránh truy cập các trang web không liên quan đến công việc và nhận biết dấu hiệu của lừa đảo và phần mềm độc hại.
- Bảo vệ Dữ liệu: Xử lý dữ liệu nhạy cảm cẩn thận, sử dụng mã hóa và thực hành chia sẻ an toàn.
- Bảo mật Thiết bị: Không chèn USB hoặc phương tiện không được ủy quyền vào thiết bị làm việc, và báo cáo ngay lập tức bất kỳ thiết bị bị mất hoặc bị đánh cắp.

1.3 Soạn thảo Chính sách Nhận thức & Đào tạo Bảo mật Toàn Tổ chức

1.4 Tổng kết

1.4.1 Tổng quan

Trong bài thực hành này, sinh viên đã xem xét và xác định các rủi ro và mối đe dọa phổ biến trong Miền Người Dùng và Miền Máy Trạm. Từ đó, các yếu tố của định nghĩa chính sách đào tạo nhận thức bảo mật được liên kết với các mục tiêu và mục đích định nghĩa chính sách. Sinh viên sau đó đã tạo định nghĩa Chính sách Nhận thức & Đào tạo Bảo mật tập trung vào các yêu cầu như được định nghĩa trong kịch bản đã cho. Chính sách này, kết hợp với nội dung đào tạo nhận thức bảo mật thực tế được tùy chỉnh cho Ngân hàng Tín dụng ABC, có thể giúp giảm thiểu các rủi ro và mối đe dọa trong Miền Người Dùng và Miền Máy Trạm và sẽ đóng góp vào chiến lược bảo mật phân tầng tổng thể của tổ chức.

1.4.2 Câu hỏi Đánh giá Bài Thực hành & Câu trả lời

- Chính sách nhận thức & đào tạo bảo mật ảnh hưởng như thế nào đến khả năng của tổ chức trong việc giảm thiểu rủi ro, mối đe dọa và lỗ hổng?

Một chính sách bảo mật xây dựng nhận thức, giảm rủi ro và lỗ hổng bằng cách khuyến khích các hành vi an toàn.

- Tại sao bạn cần một chính sách nhận thức & đào tạo bảo mật nếu bạn có nhân viên mới tham gia hoặc tham dự chương trình đào tạo nhận thức bảo mật của tổ chức trong định hướng nhân viên mới?

Chính sách liên tục củng cố nhận thức khi các mối đe dọa phát triển, vượt ra ngoài đào tạo ban đầu.

- Mối quan hệ giữa Chính sách Sử dụng Chấp nhận được (AUP) và Chính sách Nhận thức & Đào tạo Bảo mật là gì?

AUP định nghĩa quy tắc sử dụng; chính sách bảo mật dạy các thực hành an toàn và phản ứng với rủi ro.

- Tại sao quan trọng để ngăn chặn người dùng tham gia vào việc tải xuống hoặc cài đặt ứng dụng và phần mềm tìm thấy trên Internet?

Ngăn chặn phần mềm độc hại và phần mềm không được phê duyệt làm tổn hại đến bảo mật.

- Khi cố gắng chống lại lỗ hổng phần mềm trong Miền Máy Trạm, điều gì cần thiết nhất để xử lý hệ điều hành, ứng dụng và các cài đặt phần mềm khác?

Vá lỗi và cập nhật định kỳ bảo vệ chống lại các lỗi phần mềm.

- Tại sao quan trọng để giáo dục người dùng về các rủi ro, mối đe dọa và lỗ hổng tìm thấy trên Internet và web toàn cầu?

Giúp người dùng nhận biết và tránh các mối đe dọa dựa trên web phổ biến.

- Các chiến lược nào để ngăn chặn người dùng hoặc nhân viên tải xuống và cài đặt ứng dụng và phần mềm rogue tìm thấy trên Internet?

Sử dụng kiểm soát ứng dụng, quyền hạn chế và phần mềm bảo mật.

-. Chiến lược nào để ngăn chặn người dùng nhấp vào tệp đính kèm e-mail và tệp không xác định?

Các bài kiểm tra lừa đảo và đào tạo giảm hành vi e-mail rủi ro.

-. Tại sao kỹ thuật xã hội nên được bao gồm trong đào tạo nhận thức bảo mật?

Trao quyền cho nhân viên nhận biết các chiến thuật thao túng.

-. Hai miền nào của một cơ sở hạ tầng CNTT điển hình là trọng tâm của Chính sách Nhận thức & Đào tạo Bảo mật?

Tập trung vào Miền Người Dùng và Miền Máy Trạm.

- Tại sao nên bao gồm các chính sách toàn tổ chức trong đào tạo nhận thức bảo mật của nhân viên?

Đảm bảo hiểu biết nhất quán về trách nhiệm bảo mật.

- Miền nào thường đóng vai trò là điểm vào của cơ sở hạ tầng CNTT?

Miền Người Dùng là điểm vào ban đầu

Miền nào thường đóng vai trò là điểm vào của hệ thống, ứng dụng, cơ sở dữ liệu của cơ sở hạ tầng CNTT?

Miền Máy Trạm truy cập hệ thống

-. Tại sao một tổ chức cần chính sách về việc tiến hành đào tạo nhận thức bảo mật hàng năm và định kỳ?

Đào tạo định kỳ giữ kiến thức bảo mật cập nhật.

- Các chiến lược khác nào mà tổ chức có thể triển khai để giữ nhận thức bảo mật luôn ở mức cao với tất cả nhân viên và người dùng được ủy quyền?

Sử dụng nhắc nhở, mô phỏng lừa đảo và cập nhật định kỳ.

-. Tại sao một tổ chức nên cung cấp đào tạo nhận thức bảo mật cập nhật khi một chính sách mới được triển khai xuyên suốt Miền Người Dùng hoặc Miền Máy Trạm?

Đảm bảo nhân viên được thông báo về các thay đổi giao thức.