TẤN CÔNG MẠNG

ĐÓ LÀ GÌ

Không như các mối đe dọa thể chất thúc đẩy hành động ngay lập tức, các mối đe dọa và tấn công mạng thường khó xác định hoặc nhận thức được. An ninh mạng liên quan đến việc ngăn chặn, dò tìm và ứng phó với các sự cố mạng. Hầu như tất cả các tổ chức hiện đại – bao gồm chính phủ, bệnh viện, tập đoàn, ngân hàng và tiện ích – đều dựa vào hệ thống máy tính để vận hành và quản lý dữ liệu, do đó dễ bị tấn công mạng.

Cái gọi là "tấn công bề mặt", có thể dễ bị tấn công bởi các tác nhân xấu có thể bao gồm phần cứng máy tính, máy tính bảng, điện thoại và nhiều thiết bị và ứng dụng hỗ trợ duyệt web khác trong hệ thống mạng được gọi là "Internet Vạn Vật". Trong số các mối nguy hiểm của các cuộc tấn công mạng là kẻ xâm nhập xóa toàn bộ hệ thống, nắm giữ dữ liệu hoặc hệ điều hành để đòi tiền chuộc, đánh cắp thông tin bí mật hoặc cá nhân, xâm nhập vào hệ thống và thay đổi tập tin hoặc sử dụng máy tính hay thiết bị để truy cập danh sách liên lạc và tấn công hoặc lây nhiễm cho người khác.

THUẬT NGỮ CHÍNH

- **Cuộc Tấn Công Mạng** có thể bắt nguồn từ các cá nhân, nhóm làm việc trên mạng, nhóm khủng bố, hoặc các quốc gia, và có thể gây ra các vấn đề nghiêm trọng (và nguy hiểm) cho chính phủ, doanh nghiệp, các tiện ích và công chúng.
- **Xâm Nhập** là một cuộc tấn công trực tiếp vào hệ thống "thông qua các dây dẫn" trong đó kẻ tấn công (là người sống hoặc là một "máy" tự động) đạt được quyền truy cập trực tiếp vào dữ liệu hoặc hoạt động được bảo mật/hạn chế. Thông thường, các lối đi cho phép xâm nhập như vậy được mở ra thông qua "trò lừa đảo trực tuyến" hoặc tải xuống.
- **Internet Vạn Vật (IoT)** bao gồm các thiết bị và công cụ được hỗ trợ bằng mạng như tủ lạnh, hệ thống loa, đồng hồ, rơ le nhiệt, hệ thống an ninh, máy pha cà phê, v.v…
- **Tấn Công Giả Mạo Trên Mạng** bao gồm các hình thức liên lạc phổ biến rộng rãi bằng email hoặc tin nhắn với hy vọng rằng một vài người nhận sẽ bấp vào đâu đó trong tin nhắn (ví dụ: tập tin đính kèm, liên kết, nút bật "kích hoạt macro") kích hoạt virus hoặc phần mềm độc hại khác. Chiến dịch tấn công giả mạo trên mạng có mục tiêu – ví dụ: chống lại một chính phủ hoặc tiện ích cụ thể – được gọi là lừa đảo trực tuyến.
- **Tấn Công Phi Kỹ Thuật** liên quan đến việc khai thác các lỗ hổng của người dùng thay vì hệ thống của họ, để phá vỡ các biện pháp bảo mật CNTT. Ví dụ bao gồm tấn công giả mạo trên mạng, lừa đảo qua email và các khuyết điểm khác. Người dùng thường là yếu tố dễ bị đánh bại nhất trong kiến trúc bảo mật CNTT.

ĐIỀU CẦN LÀM

Trước khi xảy ra (Chuẩn bị sẵn sàng/Giảm thiểu)

- ❑ Luôn bật tường lửa của quý vị và cập nhật.
- ❑ Cài đặt hoặc cập nhật phần mềm chống vi-rút/phần mềm chống gián điệp.
- ❑ Dùng mật khẩu đặc biệt, độc nhất, khó đoán và thay đổi chúng một cách thường xuyên.
- ❑ Tìm kiếm và cài đặt kịp thời tất cả các bản cập nhật cho hệ thống điều hành firmware, phần mềm và phần mềm chống vi-rút của quý vị.
- ❑ Cẩn thận với những gì quý vị tải xuống. Tuyệt đối không bấm vào tập tin đính kèm, liên kết hoặc macro trong email hoặc tin nhắn không được yêu cầu.
- ❑ Tắt máy tính khi quý vị không sử dụng.
- ❑ Luôn xác minh nguồn email và nếu nghi ngờ hãy xóa chúng.
- ❑ Cảnh giác với email từ các địa chỉ liên lạc đã biết có vẻ "đáng nghi" – như lỗi chính tả, syntax khó hiểu hoặc cách sử dụng từ, ngôn ngữ chung, URL liên kết lạ – nhiều chiến dịch hack sẽ mạo danh các email đã biết của quý vị.
- ❑ Chụp ảnh màn hình các nội dung đáng ngờ trước khi xóa nó để có thể phân tích.
- ❑ Thường xuyên sao lưu tất cả dữ liệu của quý vị vào ổ cứng ngoài hoặc Cloud; bật tính năng "Time Machine" nếu quý vị sử dụng dòng máy Mac.

Trong khi (Ứng phó)

- ❑ Ngắt kết nối thiết bị bị nhiễm khỏi mạng của quý vị.
- ❑ Nếu quý vị đang ở nơi làm việc, hãy thông báo cho nhân viên IT về bất kỳ cuộc tấn công đáng ngờ hoặc đã được xác nhận nào trên thiết bị của quý vị và cung cấp ảnh chụp màn hình.
- ❑ Nếu một sự kiện xảy ra dẫn đến mất thông tin tài chính, cá nhân hoặc hồ sơ y tế, hãy trình báo cảnh sát.

Sau khi (Phục hồi)

- ❑ Thông báo cho bất kỳ ai có thể bị ảnh hưởng xấu, bao gồm tài khoản tín dụng, tài khoản ngân hàng, khách hàng, chủ lao động, gia đình và bạn bè của quý vị. Thay đổi tài khoản của quý vị và tất cả mật khẩu.
- ❑ Chạy chương trình quét và tiện ích thích hợp để loại bỏ việc lây nhiễm bất kỳ.
- ❑ Theo dõi báo cáo tín dụng, báo cáo ngân hàng, các khoản đầu tư và bản sao kê thẻ tín dụng của quý vị.
- ❑ Đảm bảo thiết bị của quý vị không bị nhiễm, và hãy xóa sạch ổ cứng và cài đặt lại tất cả phần mềm nếu có bất kỳ nghi ngờ nào.