Tìm hiểu về chuẩn SMTP STS – chuẩn bảo mật Email mới hỗ trợ cho chuẩn cũ StartTLS

Nguyễn Hồng Sơn
Kiến thức - 01/04/2016

Bên cạnh rất nhiều ứng dụng nhắn tin nhanh, Email vẫn là một trong những cách giao tiếp phổ biến nhất trong thời đại số hiện nay. Nhưng liệu rằng Email của bạn có an toàn? Chuẩn SMTP STS đã được phát minh để giải quyết vấn đề chuẩn cũ kém bảo mật StartTLS.

Chúng ta đã sử dụng dịch vụ email được vài thập kỉ, nhưng giao thức truyền tải email là Simple Mail Transfer Protocol (SMTP) đã cũ và thiếu khả năng đảm bảo an toàn cho email. Để cải thiện vấn đề này, SMTP STARTTLS đã được phát minh vào năm 2002 như một bản nâng cấp dành cho kết nối kém bảo mật thành kết nối an toàn sử dụng TLS. Nhưng STARTTLS cũng rất dễ bị khai thác bằng kỹ thuật tấn công Man-in-the-Middle (MitM) nhằm làm suy yếu khả năng mã hóa.

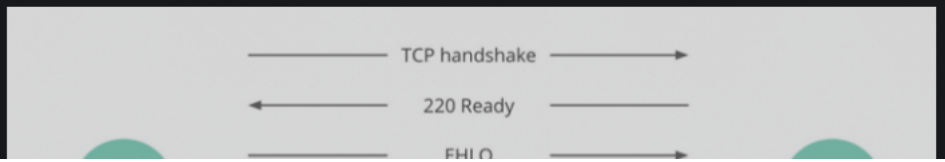
Các nhà cung cấp dịch vụ email hàng đầu như Google, Microsoft, Yahoo!, Comcast, LinkedIn, và 1&1 Mail & Media Development, đã hợp tác phát triển một chuẩn gửi thư điện tử mới, đảm bảo email được gửi thông qua kênh mã hóa và không thể bị đánh cắp. Chuẩn email mới này có tên **SMTP Strict Transport Security** (SMTP STS) sẽ thay đổi cách người dùng sử dụng hòm thư.

SMTP STS được thiết kế nhằm nâng cao giao thức kết nối an toàn cho email. Giao thức này đã được trình lên tổ chức Internet Engineering Task Force (IETF – tổ chức có chức năng nghiên cứu, phát triển và quyết định các chuẩn dùng trong Internet) vào thứ sáu tuần trước để ban hành sử dụng. Mục đích chính của SMTP STS là ngăn chặn tấn công MitM có thể vượt qua chuẩn cũ kém bảo mật như STARTTLS.

Tại sao StartTLS lại không thể đảm bảo an toàn cho Email?

Đây là câu hỏi các bạn nên quan tâm và tìm câu trả lời. STARTTLS rất dễ bị khai thác bởi kỹ thuật tấn công MitM nhằm làm khả năng mã hoá bị suy yếu do đó giao thức này không thể đảm bảo cơ chế bảo mật cho thông điệp hay xác thực cho máy chủ. Cơ chế hoạt động của giao thức này như sau:

> **Đọc thêm:** Những điều cần biết về chữ ký số



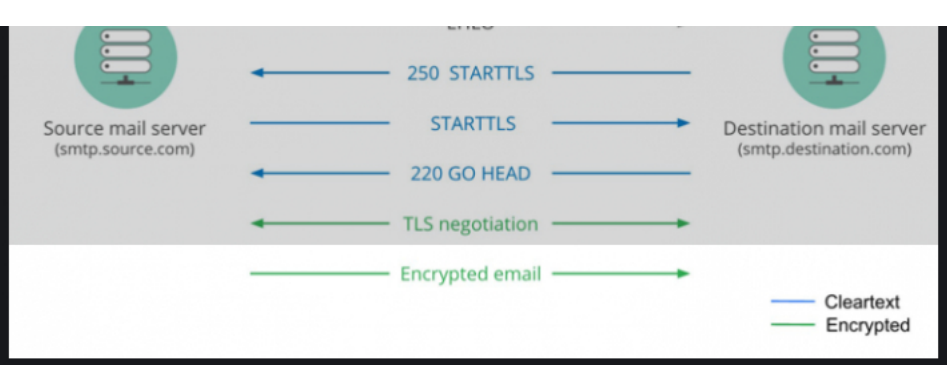
Bài viết nổi bật

Thế giới đã sẵn sàng cho cuộc đại tấn công của mã độc tống t...
Tấn công mạng - 22/03/2019

7 mối đe dọa về bảo mật trong các thiết bị di động năm 2019
Tin tức - 21/03/2019

Quyền riêng tư của bạn có bị xâm hại khi bạn là "công dân mẻ...
Cộng đồng - 19/03/2019

MongoDB tiết lộ dữ liệu giám sát của Trung Quốc
Lỗ hổng - 05/03/2019



Khi một client ping đến máy chủ Email, client sẽ hỏi máy chủ Email có hỗ trợ SSL hay không. Tại đây, tin tặc có thể can thiệp vào quá trình "bắt tay" này và làm Client tin rằng máy chủ Email không hỗ trợ SSL. Điều này đồng nghĩa với việc tin tặc có thể làm suy yếu khả năng mã hoá TLS hoặc thậm trí có thể đọc, sửa được nội dung Email khi Client đã bị thuyết phục và thoả hiệp khi gửi thư trong trạng thái không được mã hoá (Cleartext Content).

SMTP STS đảm bảo an toàn cho email hơn StartTLS như thế nào?

SMTP Strict Transport Security được thiết kế làm việc cùng với StartTLS để tăng tính bảo mật cho giao thức SMTP nhằm chống lại khả năng làm suy yếu mã hoá từ kỹ thuật tấn công MitM hoặc sửa đổi mail giữa các thiết bị đầu cuối hỗ trợ STARTTLS. SMTP STS hoạt động dựa trên xác nhận chứng chỉ được nhận dạng bởi TLS hoặc DANE TLSA. Chuẩn bảo mật mới này sẽ kiểm tra liệu người nhận email có hỗ trợ SMTP STS hay không và nếu hợp lệ sẽ cập nhật chứng chỉ mã hóa. Email sau đó sẽ được gửi đi. Trong trường hợp email không gửi được, sẽ có thông báo lí do tới người dùng.

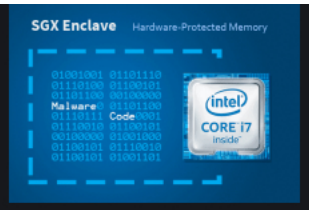
Chuẩn bảo mật mới SMTP STS đã được trình lên tổ chức IETF và đợi phê duyệt. Sẽ phải mất 6 tháng để IETF xem xét trước khi ban hành sử dụng và đưa nó vào thực tiễn. Trong thời gian này, tốt nhất bạn nên sử dụng các dịch vụ mã hóa email miễn phí, mã nguồn mở như **ProtonMail** để giúp email luôn được an toàn.

THN

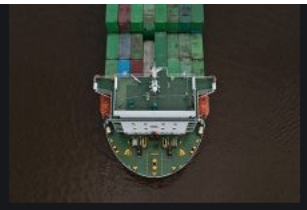
#Bảo mật #Công nghệ mới #mã hóa email #SMTP STS

Nguyễn Hồng Sơn

BÀI VIẾT LIÊN QUAN **XEM THÊM**



Các nhà nghiên cứu cấy phần mềm độc hại trên Intel SGX Enclaves



Động cơ đầu máy bị tấn công do bảo mật bộ điều khiển kém

Những chính sách bảo mật tiện ích mở rộng Chrome Google vừa công bố