Tên: Lê Hải Đăng

MSSV: 20110243

KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)

Môn: An toàn thông tin

1. (3 điểm) Trình bày giải pháp để đảm bảo an toàn cho ứng dụng Email?

Ngày nay, các thông tin được trao đổi qua dịch vụ thư điện tử ngày càng trở nên đa dạng, phong phú và cũng kéo theo sự ra đời của nhiều cách thức, phương pháp tấn công mới nhằm phá hoại hệ thống, đánh cắp thông tin.... Do vậy, việc đảm bảo ATTT của thư điện tử là một vấn đề đang được quan tâm, đầu tư nghiên cứu của các nhà cung cấp dịch vụ thư điện tử.

Hệ thống thư điện tử thường được tổ chức theo mô hình Client/ Server, trong đó:

- Mail server có nhiệm vụ nhận thư từ Mail Client và chuyển đến Mail Server của Client đích, đồng thời lưu trữ thư điện tử được gửi đến để Client tải về. Quá trình chuyển và phân phát thư của các Mail Server không phân biệt giữa thư thường và thư mật.
- Mail Client Có nhiệm vụ gửi và nhận thư từ Mail Server. Hệ thống này có chức năng mã và ký thư trước khi gửi đi, kết nối, quản lý thư, giải mã và kiểm tra chữ ký.

Dịch vụ thư điện tử làm việc theo nguyên tắc offline. Mail Client chỉ kích hoạt khi có nhu cầu gửi, nhận thư của người sử dụng. Người dùng giao tiếp với hệ thống thư thông qua giao diện tại Mail Client. Thư được tạo ra tại Mail Client và được chuyển sang Mail Server mà Mail client kết nối tới. Trong quá trình chuyển giao đến đích, thư điện tử có thể được chuyển giao và lưu giữ tại một số Mail Server, nên khả năng bị tấn công là rất cao. Bởi vậy, hệ thống thư điện tử an toàn phải đảm bảo được các yêu cầu sau:

- Đảm bảo bí mật thông tin về tài khoản khi kết nối đến server, giúp cho thông tin về người dùng được gửi đi an toàn trong quá trình đăng nhập, giúp kiểm soát chặt chẽ và xác thực người dùng trong hệ thống.
- Mã hóa các thông điệp gửi và nhận giữa các người dùng để đảm bảo an toàn dữ liệu trên đường truyền.
- Xác thực được nội dung các thông điệp và xác thực được người gửi. Yêu cầu này đưa ra nhằm đảm bảo tính toàn vẹn của dữ liệu, chống giả mạo dữ liệu và chống chối bỏ.

Như vậy giải pháp để đảm bảo an toàn cho ứng dụng Email là gì?

a) **Bảo đảm an toàn thông tin tài khoản khi đăng nhập:**

Yêu cầu đầu tiên của bất kỳ hệ thống kiểm soát đăng nhập nào là thông tin về tài khoản, đặc biệt là mật khẩu phải được đảm bảo bí mật khi gửi qua mạng. Điều này càng quan trọng đối với hệ thống thư điện tử, vì thông tin về địa chỉ thư là công khai và khi lộ mật khẩu người dùng sẽ bị mạo danh. Mật khẩu ở dạng rõ khi gửi đi trên đường truyền tới server có thể dễ dàng bị chặn bắt và đọc trộm. Mặt khác, người dùng thường chọn các mật khẩu có ít ký tự để dễ nhớ, do đó hacker dễ đoán và thử mật khẩu để kết nối đến server. Để khắc phục những vấn đề trên, hệ thống thư mật sử dụng các hàm băm để biến đổi mật khẩu khi gửi lên server. Khi đó server sẽ tính lại giá trị băm của mật khẩu để so sánh xác thực. Như vậy, chỉ người dùng mới biết mật khẩu ở dạng rõ của mình và mật khẩu này chỉ xuất hiện khi được nhập vào ô thông tin đăng nhập.

b) Đảm bảo an toàn dữ liệu trên đường truyền

Trong dịch vụ thư điện tử, các thông tin khi gửi đi trên đường truyền có thể bị chặn bắt bất hợp pháp, do đó nguy cơ mất an toàn cho dữ liệu là rất lớn. Giải pháp được sử dụng rộng rãi nhất hiện nay cho vấn đề an toàn dữ liệu là kỹ thuật mã hóa. Trong hệ thống thư mật, nội dung của thông điệp trước khi gửi đi sẽ được mã hóa tại phía người gửi bằng một khóa phiên, sau đó nội dung thư đã được mã hóa cùng với khóa phiên (đã được mã hóa bằng khóa công khai của người nhận) sẽ được đóng gói vào khuôn dạng chuẩn và gửi đi. Tại nơi nhận, chương trình Mail Client sẽ lấy thư mật về cơ sở dữ liệu cục bộ, tách phần nội dung và tách thông tin về người gửi trong thông điệp, dùng khóa bí mật của người nhận để giải mã khóa phiên sau đó dùng khóa phiên để giải mã nội dung của thư.

c) Xác thực nội dung thông điệp và người gửi

Chữ ký số được ứng dụng trong hệ thống bảo mật thư nhằm đảm bảo toàn vẹn của thông điệp, cũng như tính xác thực và tính chống chối bỏ của thông điệp. Trước khi thư được gửi đi, chương trình Mail Client mật sẽ ký nội dung thư và các file đính kèm bằng cách tính giá trị băm của chúng và mã bằng khóa bí mật của người gửi. Chữ ký được đóng gói cùng với thư theo khuôn dạng chuẩn và gửi đến nơi nhận. Tại nơi nhận, người nhận tách phần chữ ký trong nội dung thư và các file đính kèm, sau đó dùng khóa công khai của người gửi để giải mã ra các giá trị băm, tính toán lại các giá trị băm của nội dung thư và file đính kèm, so sánh chúng với các giá trị băm đã giải mã được. Vì chữ ký được tạo bởi khóa bí mật của người gửi, không thể giả mạo được nên tính toàn vẹn của thư sẽ được đảm bảo và người gửi không thể chối bỏ các thông tin đã giao dịch.

Hệ thống bảo mật thư sẽ sử dụng hệ mật khóa công khai để phân phối khóa phiên cho các phiên làm việc và xác thực, còn hệ mật khóa đối xứng được sử dụng để mã hóa dữ liệu. Để quản lý và phân phối khóa, hệ thống bảo mật thư ứng dụng cơ sở hạ tầng khóa công khai (PKI). Mỗi thành viên tham gia vào hệ thống thư được cấp phát một cặp khóa công khai và khóa bí mật. Các khóa công khai được công bố rộng rãi thông qua chứng thư X509 V3, do đó các thành viên có thể dễ dàng có khóa công khai của nhau một cách tin cậy. Khi sử

dụng chứng thư số trong hệ thống thư mật, các cặp khóa của người dùng và khóa công khai của CA sẽ được lưu trữ trên thiết bị eToken an toàn, tiện lợi cho quá trình sử dụng. Cách phân phối khóa như trên giúp cho việc quản lý khóa và mở rộng hệ thống trở nên thuận lợi hơn, đặc biệt là đối với mạng liên lạc có nhiều người sử dụng thư điện tử.

Về phía người dùng cũng cần lưu ý các thông tin sau:

a) Sử dụng mật khẩu mạnh:

Để an toàn, mật khẩu nên có cả chữ in hoa, chữ thường, ký tự đặc biệt và số. Nhiều người có thói quen sử dụng các mật khẩu dễ nhớ như ngày sinh, tên của mình, thậm chí là mật khẩu dễ đoán như 123456, 111111…

Nếu email không có gì quan trọng, người dùng có thể sử dụng mật khẩu đó, nhưng nếu dùng để trao đổi thông tin mật, giao dịch ngân hàng… thì đó là hành động tự trao dữ liệu cho tin tặc. Bên cạnh đó, không nên sử dụng cùng một mật khẩu cho nhiều tài khoản, bởi chỉ cần biết một trong số đó, tin tặc có thể đăng nhập vào các tài khoản còn lại và đánh cắp mọi thứ.

b) Thiết đặt xác minh 2 bước:

Hiện nay, hầu hết các dịch vụ giao dịch điện tử trực tuyến đều có thêm tính năng xác thực 2 bước. Đây là biện pháp bảo mật bổ sung giúp tài khoản an toàn hơn, bởi ngoài mật khẩu thông thường, tài khoản sẽ yêu cầu thêm mã xác minh được gửi về điện thoại di động, thông qua tin nhắn SMS. Với tính năng này, kể cả khi tin tặc đánh cắp được mật khẩu vào email, chúng cũng không thể đăng nhập vào tài khoản được vì không có mã xác minh. Lúc này, người dùng có thể dễ dàng phát hiện được tài khoản của mình đang gặp nguy hiểm, điều quan trọng nhất là phải thay đổi mật khẩu ngay lập tức.

c) Không đăng nhập vào mạng wifi công cộng để gửi email quan trọng:

Wifi hiện đã có ở khắp mọi nơi, từ quán cà phê, nhà hàng, quán ăn… Không phủ nhận sự tiện lợi mà nó mang lại, tuy nhiên chúng cũng tiềm ẩn nguy cơ bị đánh cắp dữ liệu, các tài khoản trong đó có tài khoản email.

Khi đăng nhập vào mạng wifi công cộng, thiết bị của người dùng có thể bị kẻ khác trên cùng mạng đó đột nhập nếu cách bảo mật không an toàn. Nhưng ngay cả khi mã hóa bằng các giao thức bảo mật, người dùng cũng vẫn có thể bị lừa thông qua các phần mềm, liên kết độc hại. Tất nhiên, khi đột nhập thành công, không chỉ lấy cắp tài khoản email, mạng xã hội… tin tặc còn làm nhiều điều khác, như kích hoạt camera, micro để quay và nghe lén.

Theo thống kê, 1TB dữ liệu bị đánh cắp mỗi ngày, tương đương 1 tỷ người bị đánh cắp thông tin đăng nhập thông qua wifi công cộng. Do đó, không nên thực hiện các giao dịch, gửi email quan trọng trong khi đăng nhập vào mạng này. Thay vào đó, nếu cần thiết, hãy sử dụng mạng 3G/4G để được an toàn.

d) Không click vào các đường link lạ:

Đây là cách thức tấn công khá phổ biến và đã được cảnh báo từ lâu, tuy nhiên vẫn có nhiều người nhẹ dạ làm theo, hậu quả là tài khoản bị đánh cắp, trong đó có cả tài khoản email.

Cách thức tấn công của tin tặc khá đơn giản: chúng sử dụng một địa chỉ liên kết tới phần mềm độc hại nhưng "núp bóng" dưới các tiêu đề gây tò mò hoặc phần mềm tin cậy. Khi người dùng click vào đó, lập tức mã độc xâm nhập vào hệ thống mà người đó không hề hay biết. Cuối cùng, phần mềm độc hại chạy dưới nền máy tính và ghi lại những thứ người dùng nhập vào, hoặc đánh cắp dữ liệu và gửi về máy chủ từ xa.

Do đó, với các email và liên kết nghi ngờ, tốt nhất người dùng không nên click vào, hoặc xác thực độ tin cậy của nó trước khi nhấp chuột.

2. (4 điểm) Trình bày các nguyên tắc để đảm bảo an toàn cho các phần mềm ứng dụng của doanh nghiệp?

Có thể nói rằng, sống còn của doanh nghiệp/tổ chức đó chính là an ninh mạng. Nó không chỉ giúp bảo vệ những thông tin dữ liệu bí mật trước sự đe dọa thường trực của hacker mà còn giúp doanh nghiệp nâng cao hiệu quả trong sản xuất và quản lý tốt máy móc, thiết bị trong quá trình hoạt động. Quan trọng nhất là an ninh mạng giúp giảm thiểu kiểm soát được ở mức thấp nhất rủi ro mất mát hư hỏng và khả năng phục hồi của dữ liệu, giúp cho việc sản xuất hoạt động liên tục không gián đoạn. Chẳng hạn như: an ninh mạng trong công nghiệp, an ninh mạng lưới, an ninh mạng cho trung tâm dữ liệu…

Trước những mối nguy hại đó, cần có những giải pháp an ninh mạng để các phần mềm doanh nghiệp hoạt động ổn định:

a) **Cài mật khẩu cấp độ mạnh:** Đã rất nhiều chuyên gia cảnh báo về vấn đề này, nhưng nhiều doanh nghiệp vẫn xem nhẹ và đã có vài nơi phải chịu hậu quả nghiêm trọng. Quý doanh nghiệp nên nhớ rằng, đặt mật khẩu mà mật khẩu dễ đoán, lại dùng chung cho nhiều thiết bị máy móc hệ thống thì chả khác nào miếng mồi ngon để những kẻ xấu dòm ngó tài nguyên của quý vị. Kẻ xấu đã có được mật khẩu rồi thì việc xâm nhập vào toàn bộ hệ thống là quá dễ dàng. Quý doanh nghiệp cần đặt mật khẩu có độ mạnh tuyệt đối, 12 ký tự trở nên bao gồm chữ thường + chữ in hoa + con số + ký hiệu đặc biệt; mỗi thiết bị hệ thống mỗi mật khẩu khác nhau không dùng chung. Nếu việc quản lý mật khẩu khó quá thì dùng ứng dụng quản lý sẽ tiện hơn và cũng đảm bảo an toàn hơn.
b) **Cài đặt bảo mật máy tính:** Để có được một hệ thống máy tính mạnh, có sức chống chọi với những sự tấn công phá hoại từ bên ngoài, doanh nghiệp cần phải đầu tư cho việc cài đặt bảo mật cho máy tính. Thực tế hiện nay, việc 1 cá thể trong doanh nghiệp click vào 1 đường link lạ hay tải một cái gì đó về máy tính là đã có thể “rước” virus

về phá hoại rất dễ dàng. Có rất nhiều phần mềm bảo mật trả phí tốt hiện nay mà doanh nghiệp có thể cân nhắc, chẳng hạn như EDR Security Doctor.

c) **Bảo mật phần cứng:** Phần mềm xong thì doanh nghiệp phải nghĩ đến việc bảo mật phần cứng. Phần cứng bao gồm những gì ? Nói chung là tất cả thiết bị nào mà đang kết nối internet như thì là phần cứng hết : laptop, máy tính bàn, ổ đĩa, smartphone, máy tính bảng….đều phải được cài phần mềm bảo vệ và tường lửa.

d) **Bảo mật mạng theo từng cấp độ:** Nếu doanh nghiệp chỉ bảo mật theo 1 kiểu hay 1 cấp độ duy nhất là quá xem thường an ninh mạng rồi. Hacker hiện nay chỉ cần có thế thôi cũng đã đủ đánh chiếm tài nguyên doanh nghiệp rồi, vì thế phải phân cấp cho từng cấp độ mạng để lên kế hoạch bảo mật như :
   - Wifi : hiện nay hack wifi, chiếm đoạt thông tin hệ thống qua wifi đã nhan nhản khắp nơi nên doanh nghiệp cần có mạng LAN riêng để bảo mật được tốt hơn.
   - Tường lửa : tường lửa được xem là cánh cổng bảo vệ hệ thống ngay từ bên ngoài, phát đi cảnh báo khi có sự đe dọa đến máy tính.
   - Cáp Ethernet : được tạo từ một nền tảng vững chắc và được bảo mật nghiêm ngặt nên việc đánh cắp, truy cập hay phá vỡ cấu trúc là điều vô cùng khó khăn.

e) **Quản lý người dùng tốt:** Mỗi người dùng khi truy cập vào hệ thống mạng của công ty phải có tài khoản riêng để dễ theo dõi, xem rằng họ đã thao tác những gì và sau này lỡ khi họ nghỉ rồi thì người chủ có thể khóa tài khoản của họ lại được. Như vậy thì đảm bảo dữ liệu không bị tuồn ra ngoài cũng như xác định được danh tính kẻ phá hoại.

Ngoài những giải pháp đã nêu trên, chúng ta có thể quan tâm đến giải pháp MetaAccess của OPSWAT - giải pháp có thể giải quyết hầu hết các thách thức trên để đảm bảo an toàn cho các truy cập vào ứng dụng của doanh nghiệp.

Bằng cách thường xuyên theo dõi các thiết bị với chính sách bảo mật mà TC/DN đặt ra, MetaAccess cho phép các thiết bị tuân thủ được phép truy cập vào ứng dụng và ngăn chặn các thiết bị không tuân thủ truy cập. Đồng thời, đưa ra những hướng dẫn cụ thể giúp người dùng cuối có thể tự khắc phục được các vấn đề trên thiết bị của họ, như yêu cầu cập nhật phần mềm antivirus, cập nhật phần mềm khắc phục lỗ hổng bảo mật… mà vẫn có thể tiếp tục sử dụng thiết bị.

Về việc đảm bảo tuân thủ các tiêu chuẩn bảo mật, MetaAccess cung cấp hơn 70 quy tắc an toàn, phù hợp với nhu cầu và quy mô của các TC/DN. MetaAccess là một giải pháp trên đám mây, nghĩa là khách hàng không cần bỏ ra chi phí đầu tư ban đầu, với công cụ quản lý tập trung từ đám mây không đòi hỏi đội ngũ kỹ thuật chuyên môn để quản lý vận hành hệ thống. Đồng thời, cung cấp khả năng tích hợp vào các hệ thống có sẵn của khách hàng thông qua các API, từ đó giảm thiểu thời gian triển khai cho TC/DN.

Thay vì ngăn chặn hoàn toàn một thiết bị không tuân thủ các quy tắc an toàn truy cập vào hệ thống mạng, giải pháp cung cấp thông tin, hướng dẫn người dùng cuối thực hiện cách khắc phục các vấn đề trên thiết bị của họ trước khi cho phép họ truy cập lại vào ứng dụng của doanh nghiệp.

Bằng việc không sử dụng các giải pháp quản lý thiết bị di động (Mobile Device Management – MDM), hỗ trợ nhiều hệ điều hành khác nhau như Windows, Mac, Linux, Android, iOS, với một chương trình chạy ngầm (agent) nhỏ không đòi hỏi nhiều về cấu hình phần cứng, giải pháp hiện đang phục vụ tốt cho nhu cầu cài đặt trên thiết bị cá nhân.

Về việc quản lý các lỗ hổng bảo mật, Hệ thống chấm điểm an toàn OPSWAT (OPSWAT Security scoring system) sẽ phân loại độ ưu tiên của các lỗ hổng bảo mật trên hơn 20.000 ứng dụng. Từ đó, việc kiểm soát, sửa lỗi các lỗ hổng bảo mật được thực hiện dễ dàng hơn.

Với sự gia tăng số lượng mã độc một cách nhanh chóng như hiện nay, giải pháp MetaAccess tích hợp với công nghệ multi-scanning giúp khách hàng phát hiện các mối đe dọa một cách nhanh chóng bằng các công nghệ như phân tích sự lặp lại của các mối đe dọa, quét các mối đe dọa trên hơn 30 chương trình chống mã độc với độ phủ cao.

Như vậy, toàn bộ các thách thức trên đều có thể giải quyết thông qua giải pháp MetaAccess. Đây cũng là một trong những giải pháp nhận được danh hiệu giải pháp đảm bảo an toàn truy cập tốt nhất năm 2019 bởi hãng truyền thông SC Media.

MetaAccess được cung cấp bởi công ty an ninh mạng OPSWAT - một trong những công ty hàng đầu thế giới về công nghệ Deep CDR và cung cấp các giải pháp để bảo vệ cơ sở hạ tầng trọng yếu cho hơn 1.200 doanh nghiệp trên thế giới.