LÝ THUYẾT

1/ Hãy nêu các chiến lược của an toàn và bảo mật hệ thống thông tin?

- **Giới hạn quyền hạn tối thiểu (Last Privilege):** theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng
- **Bảo vệ theo chiều sâu (Defence In Depth):** Không nên dựa vào một cơ chế an toàn dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ cho nhau
- **Nút thắt (Choke Point):** Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này.
- **Điểm nối yếu nhất (Weakest Link):** Chiến lược này dựa trên nguyên tắc: "Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất"
- **Tính toàn cục:** Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.
- **Tính đa dạng bảo vệ:** Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau. Nếu không, chỉ cần có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

2/ Trình bày ngắn gọn các xu hướng tấn công hiện nay?

- **Tấn công bằng phần mềm độc hại (Malware):** Bao gồm Spyware (phần mềm gián điệp), Ransomware (mã độc tống tiền), Virus, Worm (phần mềm độc hại lây lan với tốc độ nhanh).
- **Tấn công giả mạo (Phishing):** Hacker giả mạo là ngân hàng, ví điện tử, trang giao dịch trực tuyến hoặc các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin cá nhân.

- **Tấn công vào hệ thống thông tin của các cơ quan quan trọng:** truyền thông, hàng không, năng lượng, các cơ sở y tế nhằm phá hoại, đánh cắp dữ liệu.
- **Tấn công từ chối dịch vụ (DoS và DdoS):** là "đánh sập tạm thời" một hệ thống, máy chủ hoặc mạng nội bộ

3/ Mục tiêu của an toàn và bảo mật hệ thống thông tin trong doanh nghiệp là gì? Vì sao luôn cần xác định mục tiêu trước khi ứng dụng các biện pháp đảm bảo an toàn cho HTTT doanh nghiệp?

Mục tiêu của an toàn và bảo mật hệ thống thông tin trong doanh nghiệp gồm:

- **Tính bí mật:** Đảm bảo rằng thông tin không bị truy cập bất hợp pháp.
- **Tính toàn vẹn:** Đảm bảo rằng thông tin không bị sửa đổi bất hợp pháp
- **Tính sẵn dùng:** Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
- **Tính xác thực:** Đảm bảo rằng dữ liệu nhận được chắc chắn dữ liệu gốc ban đầu.
- **Tính không thể chối bỏ:** Đảm bảo rằng người gửi hay người nhận dữ liệu không thể chối bỏ trách nhiệm sau khi đã gửi và nhận thông tin.

Việc xác định mục tiêu an toàn và bảo mật hệ thống thông tin trong doanh nghiệp có nhiều lợi ích như:

- Bảo vệ được dữ liệu nhạy cảm, tránh bị đánh cắp, sao chép, lộ ra ngoài hoặc bị sửa đổi trái phép.
- Đáp ứng được các yêu cầu về tuân thủ quy định, pháp luật, tiêu chuẩn và hợp đồng liên quan đến an toàn và bảo mật thông tin.
- Đảm bảo được tính liên tục, sẵn sàng và khả năng phục hồi của hệ thống thông tin, giảm thiểu thiệt hại do các sự cố, tấn công hay tai nạn xảy ra.

- Giảm được chi phí, rủi ro và trách nhiệm pháp lý do vi phạm an toàn và bảo mật thông tin gây ra.
- Thích ứng được với các mối đe doạ tiềm năng, nâng cao khả năng ứng phó và phòng ngừa các cuộc tấn công vào hệ thống thông tin.

4/ Bảo mật kênh truyền là gì? Vì sao cần bảo mật kênh truyền tin? Có những cơ chế bảo mật kênh truyền nào?

Bảo mật kênh truyền là việc bảo mật các dữ liệu khi chúng được truyền trên kênh truyền thông, nhằm ngăn chặn sự can thiệp, giả mạo, đánh cắp hoặc phá hủy của kẻ tấn công.

Việc bảo mật kênh truyền tin là cần thiết vì:

- Bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự "đánh cắp, ăn cắp" bởi những kẻ xấu hoặc tin tặc.
- Bảo mật tốt những dữ liệu & thông tin sẽ tránh những nguy cơ không đáng có cho chính cá nhân & doanh nghiệp của bạn.
- Thông tin mật nếu bị rò rỉ ra ngoài sẽ gây ra tổn thất nghiêm trọng về niềm tin và sức cạnh tranh giữa các tổ chức, công ty.

Cơ chế bảo mật kênh truyền có thể được phân loại theo các tầng của mô hình OSI, từ tầng vật lý đến tầng ứng dụng. Một số cơ chế bảo mật phổ biến ở mỗi tầng là:

- Tầng vật lý: mã hóa quang học, mã hóa vô tuyến, mã hóa truyền thống,…
- Tầng liên kết dữ liệu: mã hóa MAC, mã hóa WEP, mã hóa WPA,…
- Tầng mạng: mã hóa IP, VPN, tường lửa, IPS, IDS,…
- Tầng vận chuyển: mã hóa TCP, TLS, SSL, DTLS,…
- Tầng ứng dụng: mã hóa HTTP, HTTPS, SSH, SFTP, SMTP, PGP,…

5/ An toàn và bảo mật thông tin là gì? Vì sao an toàn và bảo mật thông tin lại đóng vai trò rất quan trọng trong doanh nghiệp hiện nay?

An toàn và bảo mật thông tin là việc bảo vệ thông tin khỏi sự truy cập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy trái phép. Nó bao gồm việc bảo vệ thông tin cá nhân và thông tin doanh nghiệp

An toàn và bảo mật thông tin đóng vai trò rất quan trọng trong doanh nghiệp hiện nay vì:

- Thông tin mật nếu bị rò rỉ ra ngoài sẽ gây ra tổn thất nghiêm trọng về niềm tin và sức cạnh tranh giữa các tổ chức, công ty.
- Một môi trường thông tin an toàn, sạch sẽ có tác động không nhỏ đến giảm thiểu chi phí quản lý và hoạt động của doanh nghiệp, nâng cao uy tín của doanh nghiệp, tạo điều kiện thuận lợi cho sự hội nhập một môi trường thông tin lành mạnh.
- Bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự "đánh cắp, ăn cắp" bởi những kẻ xấu hoặc tin tặc.
- Ngăn chặn tin tặc đánh cắp danh tính, cài các phần mềm độc hại vào hệ thống doanh nghiệp.
- Đảm bảo những trao đổi thông tin dữ liệu, giao dịch, kinh doanh online ở trạng thái an toàn nhất

6/ Tấn công từ chối dịch vụ là gì? Trình bày đặc trưng của các kiểu tấn công từ chối dịch vụ phổ biến hiện nay? Vì sao tấn công từ chối dịch vụ rất khó phòng tránh?

Tấn công từ chối dịch vụ (DoS hoặc DDoS) là sự cố gắng ác ý của một người hay nhiều người nhằm để gián đoạn, không thể sử dụng hoặc làm cho hệ thống mạng đó chậm

đi một cách đáng kể đối với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Có năm đặc trưng cơ bản của các kiểu tấn công từ chối dịch vụ như sau:

- Nhằm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý.
- Phá vỡ các thông tin cấu hình như thông tin định tuyến.
- Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
- Phá vỡ các thành phần vật lý của mạng máy tính.
- Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.

Ngoài ra, còn có ba loại tấn công từ chối dịch vụ phổ biến là:

- Volume-based attacks: Loại tấn công sử dụng lưu lượng truy cập cao để làm ngập băng thông mạng
- Protocol attacks: Loại tấn công tập trung vào việc khai thác nguồn tài nguyên máy chủ
- Application attacks: Tấn công nhắm vào các ứng dụng web và được coi là một loại tấn công tinh vi và nghiêm trọng nhất.

Một số ví dụ về các hình thức tấn công từ chối dịch vụ là SYN Flood, UDP Flood, ICMP Flood, Ping of Death, Smurf Attack, Fraggle Attack, Teardrop Attack, Slowloris, NTP Amplification, HTTP Flood,…

Tấn công từ chối dịch vụ rất khó phòng tránh vì:

- Mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng truy cập thông thường sẽ rất khó khăn.
- Rất khó có thể tìm ra máy tính của hacker từ những request gửi tới máy chủ dịch vụ.
- Khó phân biệt và loại bỏ được các truy cập gây tổn hại tới hoạt động của máy chủ dịch vụ.
- Tấn công DDoS nhiều khi được sử dụng để che dấu cuộc tấn công mạng phía sau.

7/ Thế nào là truyền tin an toàn? Trình bày mô hình truyền tin an toàn?

Truyền tin an toàn là quá trình truyền tải thông tin một cách bảo mật và đảm bảo tính toàn vẹn của thông tin. Mô hình truyền tin an toàn là một hệ thống các phương pháp, kỹ thuật, quy trình và công nghệ được sử dụng để đảm bảo an toàn và bảo mật thông tin trong quá trình truyền tải.

Mô hình truyền tin an toàn bao gồm các thành phần chính sau:

- **Người dùng:** Là người sử dụng thông tin và có trách nhiệm đảm bảo an toàn thông tin trong quá trình truyền tải.
- **Thiết bị:** Là các thiết bị được sử dụng để truyền tải thông tin, bao gồm các thiết bị mạng, máy tính, điện thoại di động, máy tính bảng,…
- **Phần mềm:** Là các phần mềm được sử dụng để mã hóa, giải mã, xác thực và kiểm tra tính toàn vẹn của thông tin.
- **Mạng:** Là một hệ thống các thiết bị được kết nối với nhau để truyền tải thông tin.
- **Quy trình:** Là các quy trình được thiết lập để đảm bảo an toàn và bảo mật thông tin trong quá trình truyền tải.

8/ Trình bày các ứng dụng của mã hóa khóa công khai hiện nay? Cho ví dụ? Hãy phân tích những lợi điểm của mã hóa khóa công khai trong bảo mật dữ liệu?

Mã hóa khóa công khai (PKC) là một phương pháp mã hóa thông tin được sử dụng rộng rãi hiện nay. Các ứng dụng của PKC bao gồm:

- **Mã hóa dữ liệu:** PKC cho phép mã hóa dữ liệu một cách an toàn và bảo mật, đảm bảo rằng chỉ người có khóa bí mật mới có thể giải mã dữ liệu.
- **Xác thực người dùng:** PKC được sử dụng để xác thực người dùng trong các hệ thống mạng, đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào hệ thống.
- **Tạo chữ ký số:** PKC cho phép tạo chữ ký số để kiểm tra tính toàn vẹn của thông tin, đảm bảo rằng thông tin không bị thay đổi trong quá trình truyền tải.
- **Thỏa thuận khóa:** PKC được sử dụng để thiết lập khóa dùng để trao đổi thông tin mật giữa hai bên.

Ví dụ: Khóa công khai được sử dụng để mã hóa email, đảm bảo tính bảo mật của thông tin trong quá trình truyền tải.

Lợi điểm của PKC trong bảo mật dữ liệu bao gồm:

- **Không cần chia sẻ khóa bí mật:** PKC không yêu cầu chia sẻ khóa bí mật giữa các bên truyền tải thông tin, giúp đảm bảo tính riêng tư và bảo mật của thông tin.
- **Không cần sử dụng kênh truyền an toàn:** PKC cho phép truyền tải thông tin một cách an toàn và bảo mật trên các kênh truyền thông không an toàn.
- **Không cần sử dụng phần mềm bảo mật:** PKC không yêu cầu sử dụng phần mềm bảo mật để mã hóa và giải mã thông tin, giúp đơn giản hóa quá trình truyền tải thông tin.

Tuy nhiên, PKC cũng có một số nhược điểm, bao gồm:

- **Tốc độ chậm:** PKC có tốc độ chậm hơn so với các phương pháp mã hóa khác, đặc biệt là khi mã hóa các tệp tin lớn.
- **Khó triển khai:** PKC có thể khó triển khai và cấu hình đúng cách, đặc biệt là đối với các hệ thống lớn và phức tạp.
- **Khả năng bị tấn công:** PKC có thể bị tấn công bởi các kẻ xâm nhập thông qua các phương pháp như tấn công brute force hoặc tấn công giả mạo chứng chỉ SSL/TLS.

9/ Chữ ký số là gì? Trình bày các ứng dụng của chữ ký số? Nêu các đặc điểm của chữ ký số? Cho ví dụ minh họa.

Chữ ký số là một dạng trong chữ ký điện tử, có thể dùng để thực hiện giao dịch, giúp tiết kiệm chi phí và tinh gọn trong việc trình kí. Các loại chữ ký số có thể được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó có thể xác định chính xác và bảo mật.

Các ứng dụng của chữ ký số bao gồm:

- Sử dụng thay thế chữ ký tay trong tất cả các trường hợp giao dịch thương mại điện tử trong môi trường số (kê khai thuế, giao dịch ngân hàng, kí hợp đồng, văn bản, hóa đơn…).
- Trao đổi dữ liệu giữa cá nhân – tổ chức nhà nước, dễ dàng, nhanh chóng và đảm bảo tính pháp lý, tiết kiệm rất nhiều thời gian, không mất thời gian.
- Không còn phải in ấn và quản lý tài liệu giấy.
- Đảm bảo tính chính xác, toàn vẹn, bảo mật dữ liệu.

Chữ ký số có nhiều đặc điểm như sau:

- Chữ ký số có tính pháp lý cao, được thừa nhận bởi các cơ quan nhà nước và các tổ chức quốc tế.

- Chữ ký số giúp bảo vệ thông tin khỏi việc bị thay đổi, đánh cắp hoặc giả mạo bởi bên thứ ba.
- Chữ ký số cho phép thực hiện các giao dịch thương mại điện tử nhanh chóng, tiết kiệm chi phí và thời gian.
- Chữ ký số có thể áp dụng với nhiều loại dữ liệu khác nhau, như văn bản, hình ảnh, video, âm thanh, hóa đơn, hợp đồng, kê khai thuế,…

Ví dụ về chữ ký số:

- Khi bạn muốn gửi một hóa đơn điện tử cho khách hàng của mình. Bạn có thể sử dụng chữ ký số để xác nhận rằng hóa đơn đó do bạn tạo ra và không bị thay đổi bởi bất kỳ ai khác.
- Khi bạn muốn gửi một email cho một người bạn. Bạn có thể sử dụng chữ ký số để xác nhận rằng email đó do bạn gửi.

10/ Tường lửa là phần mềm gì? Tại sao cần cài đặt phần mềm tường lửa cho máy tính cá nhân của bạn?

Tường lửa là một phần mềm được sử dụng để bảo vệ máy tính khỏi các cuộc tấn công mạng từ bên ngoài. Nó hoạt động như một rào chắn giữa máy tính của bạn và Internet, kiểm soát lưu lượng truy cập vào và ra khỏi máy tính của bạn.

Tường lửa giúp bảo vệ máy tính của bạn khỏi các cuộc tấn công mạng, virus, phần mềm độc hại và các mối đe dọa khác từ Internet. Nó cũng giúp bảo vệ thông tin cá nhân của bạn khỏi việc truy cập trái phép. Cài đặt phần mềm tường lửa cho máy tính cá nhân của bạn là rất cần thiết để đảm bảo an toàn và bảo mật thông tin của bạn trên mạng.

11/ Trình bày sơ đồ mã hóa khóa đối xứng? Nêu các ứng dụng của mã hóa khóa đối xứng hiện nay? Cho ví dụ minh họa.

Sơ đồ mã hóa đối xứng thường sử dụng một khóa đơn được chia sẻ giữa 2 hoặc nhiều người dùng với nhau. Khóa duy nhất này sẽ được dùng cho cả 2 tác vụ mã hóa và giải mã các văn bản thô. Mức độ bảo mật của các hệ thống mã hóa đối xứng sẽ phụ thuộc vào độ khó trong việc suy đoán ngẫu nhiên ra khóa đối xứng theo hình thức tấn công brute force.

Các ứng dụng của mã hóa khóa đối xứng bao gồm:

- Bảo mật lưu lượng truy cập internet.
- Bảo vệ dữ liệu lưu trữ trên các máy chủ điện toán đám mây.
- Ngăn chặn gian lận trong các ứng dụng thanh toán và giao dịch thẻ.
- Xác thực danh tính của người gửi tin nhắn.

Ví dụ về mã hóa khóa đối xứng:

- Mã hóa đối xứng được sử dụng trong các hệ thống mạng máy tính.
- Mã hóa đối xứng được sử dụng trong các ứng dụng thanh toán trực tuyến.
- Mã hóa đối xứng được sử dụng trong các hệ thống lưu trữ đám mây.

12/ Mã hóa dữ liệu là gì? Khi nào cần mã hóa dữ liệu? Trình bày các ứng dụng của mã hóa dữ liệu?

Mã hóa dữ liệu là một phương pháp bảo vệ thông tin bằng cách chuyển đổi thông tin từ dạng có thể đọc và hiểu được thông thường sang dạng thông tin không thể hiểu theo các thông thường chỉ có người có quyền truy cập vào khóa giải mã hoặc có mật khẩu mới có thể đọc được nó.

Việc mã hóa dữ liệu được sử dụng để bảo vệ dữ liệu số khi nó được lưu trữ trên các hệ thống máy tính và truyền qua Internet hay các mạng máy tính khác. Các thuật toán mã hóa thường cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi.

Các ứng dụng của mã hóa dữ liệu bao gồm:

- Bảo vệ thông tin cá nhân, thông tin tài khoản ngân hàng, thông tin thẻ tín dụng, thông tin đăng nhập, thông tin giao dịch, và thông tin khác trên mạng internet.
- Bảo vệ thông tin quan trọng của chính phủ, quân đội, và các tổ chức khác.
- Bảo vệ thông tin trên các thiết bị lưu trữ như USB, ổ cứng, và các thiết bị di động khác.
- Bảo vệ thông tin trên các hệ thống máy tính và truyền qua Internet hay các mạng máy tính khác.
- Bảo vệ thông tin trên các ứng dụng tin nhắn như Facebook, WhatsApp, và các ứng dụng khác.

13/ Trình bày các nguy cơ mất an toàn trong HTTT thương mại điện tử? Vì sao các HTTT thương mại điện tử lại dễ bị tấn công hơn các HTTT khác?

Các nguy cơ mất an toàn trong HTTT thương mại điện tử:

- **Gian lận thanh toán:** Đây là hình thức mà kẻ gian hoặc hacker lợi dụng lỗi của hệ thống thanh toán để thực hiện những giao dịch ảo dẫn tới thất thoát lớn cho doanh nghiệp TMĐT.
- **Phần mềm độc hại, vi rút và gian lận trực tuyến:** Các phần mềm độc hại, vi rút và gian lận trực tuyến có thể tấn công vào hệ thống TMĐT, đánh cắp thông tin khách hàng và gây thiệt hại cho doanh nghiệp.

- **Thiếu tin tưởng vào quyền riêng tư và bảo mật:** Khách hàng có thể không tin tưởng vào quyền riêng tư và bảo mật của doanh nghiệp TMĐT, dẫn đến sự mất an toàn của thông tin khách hàng.

Các HTTT TMĐT dễ bị tấn công hơn các HTTT khác vì:

- **Số lượng người dùng lớn:** Số lượng người dùng của các HTTT TMĐT lớn hơn các HTTT khác, do đó, các tấn công mạng có thể gây ra thiệt hại lớn hơn.
- **Các giao dịch trực tuyến:** Các HTTT TMĐT thường có nhiều giao dịch trực tuyến, do đó, các tấn công mạng có thể dễ dàng xâm nhập vào hệ thống.

14/ Các yêu cầu an toàn bảo mật đối với một HTTT trong doanh nghiệp là gì? Cho ví dụ minh họa.

Các yêu cầu an toàn bảo mật đối với một hệ thống thông tin trong doanh nghiệp bao gồm:

- **Bảo mật dữ liệu:** Đảm bảo rằng dữ liệu được lưu trữ và truyền tải an toàn, không bị đánh cắp hoặc thay đổi bởi bên thứ ba. Ví dụ, mã hóa dữ liệu trước khi lưu trữ hoặc truyền tải.
- **Bảo mật hệ thống:** Đảm bảo rằng hệ thống được bảo vệ khỏi các cuộc tấn công từ bên ngoài hoặc bên trong. Ví dụ, cài đặt phần mềm chống virus và tường lửa.
- **Bảo mật truy cập:** Đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào hệ thống. Ví dụ, sử dụng mật khẩu mạnh và xác thực hai yếu tố.
- **Bảo mật vật lý:** Đảm bảo rằng các thiết bị lưu trữ dữ liệu và hệ thống máy tính được bảo vệ khỏi mất mát hoặc trộm cắp. Ví dụ, cài đặt hệ thống báo động và giám sát video.
- **Bảo mật liên tục:** Đảm bảo rằng hệ thống được bảo vệ khỏi các cuộc tấn công liên tục và được cập nhật để đối phó với các mối đe dọa mới. Ví dụ, cập nhật phần mềm và thực hiện kiểm tra bảo mật định kỳ.

15/ Phân quyền người dùng là gì? Vì sao trong HTTT doanh nghiệp cần phân quyền người dùng?

Phân quyền người dùng là một phương pháp quản lý quyền truy cập vào các tài nguyên của hệ thống thông tin, giúp đảm bảo an toàn và bảo mật thông tin của doanh nghiệp, giảm thiểu rủi ro về bảo mật thông tin và giảm thiểu thiệt hại cho doanh nghiệp, đồng thời giúp tăng hiệu quả và năng suất làm việc của nhân viên.

Trong HTTT doanh nghiệp, phân quyền người dùng là cần thiết để đảm bảo an toàn và bảo mật thông tin của doanh nghiệp. Nó giúp ngăn chặn nhân viên không có quyền truy cập vào các tài nguyên mà họ không được phép truy cập, giảm thiểu rủi ro về bảo mật thông tin và giảm thiểu thiệt hại cho doanh nghiệp.

Ví dụ cụ thể về phân quyền người dùng trong HTTT doanh nghiệp:

- Phân quyền theo chức năng: Người quản trị hệ thống có thể cấp quyền truy cập cho người dùng dựa trên chức năng của họ trong tổ chức. Ví dụ, một nhân viên kế toán có thể được cấp quyền truy cập vào các tài liệu tài chính, trong khi một nhân viên bán hàng không có quyền truy cập vào các tài liệu này.
- Phân quyền theo vai trò: Người quản trị hệ thống có thể cấp quyền truy cập cho người dùng dựa trên vai trò của họ trong tổ chức. Ví dụ, một quản lý có thể được cấp quyền truy cập vào các tài liệu quản lý, trong khi một nhân viên không có quyền truy cập vào các tài liệu này.
- Phân quyền theo đối tượng: Người quản trị hệ thống có thể cấp quyền truy cập cho người dùng dựa trên đối tượng mà họ đang làm việc. Ví dụ, một nhân viên chỉ có thể truy cập vào các tài liệu liên quan đến dự án mà họ đang tham gia.