ĐẠI NAM
UNIVERSITY

Bài 10

AN NINH MẠNG

(TẤN CÔNG MẠNG)

Giảng viên: TS. Trần Quý Nam
(namtq@dainam.edu.vn)

1. Giới thiệu về an ninh mạng

2. Các lớp bảo đảm an ninh mạng

3. Một số phương thức tấn công mạng

AN NINH MẠNG LÀ GÌ?

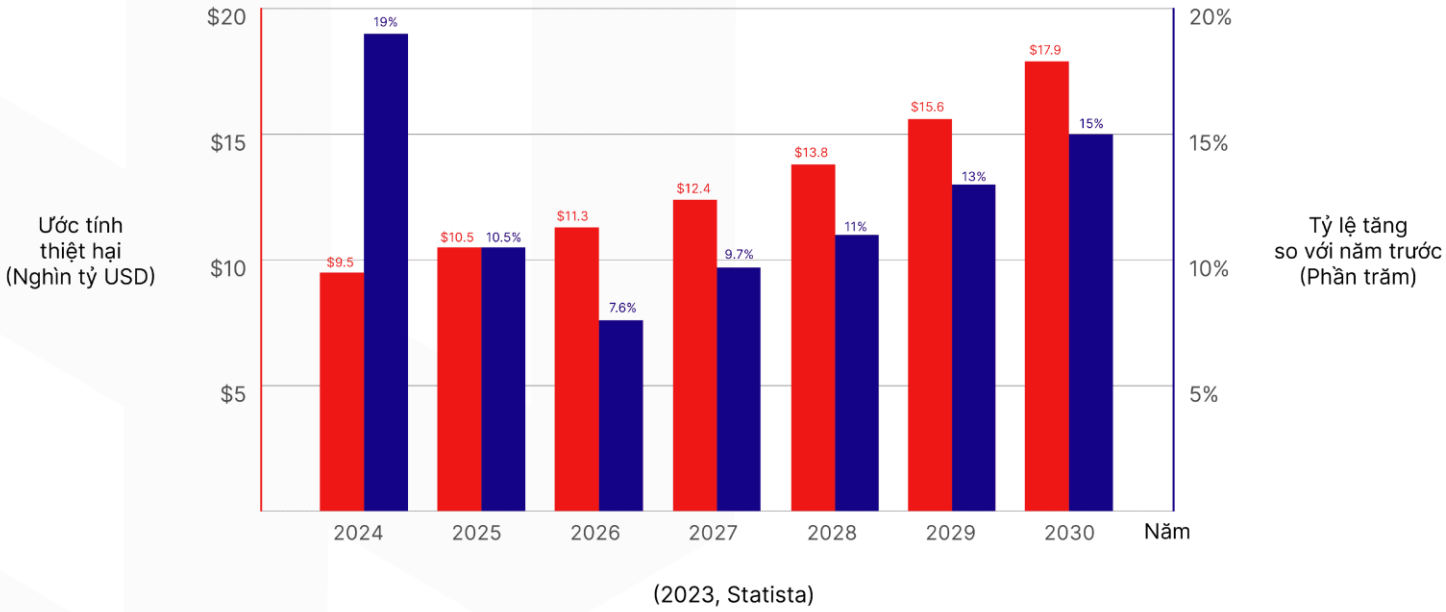
An ninh mạng (Cyber security) là tập hợp các biện pháp nhằm bảo vệ hệ thống, mạng và dữ liệu khỏi các cuộc tấn công từ không gian mạng, qua đó đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin số.

LÝ DO MẤT AN NINH MẠNG GIA TĂNG

- Hoạt động trên môi trường số tăng
- Hoạt động trên không gian mạng tăng
- Mất an toàn và lừa đảo trên mạng tăng

THIỆT HẠI TỪ MẤT AN NINH MẠNG

VNETWORK
safe and saved



(2023, Statista)

ĐẠI NAM UNIVERSITY

TÌNH HÌNH AN NINH MẠNG

HIỆP HỘI AN NINH MẠNG QUỐC GIA
NHẬN ĐỊNH VÀ DỰ BÁO TÌNH HÌNH AN NINH MẠNG NĂM 2025

Báo cáo mới nhất từ Hiệp hội An ninh mạng Quốc gia cho thấy, năm 2024 ghi nhận hơn 659.000 vụ tấn công mạng, trong đó các hình thức mã độc tống tiền và tấn công có chủ đích chiếm tỷ lệ cao nhất. Nhiều cơ quan, doanh nghiệp bị gián đoạn hoạt động, thiệt hại không chỉ tính bằng tiền mà còn làm uy tín suy giảm nghiêm trọng.

Theo báo cáo của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an, chỉ tính riêng các đơn vị trọng yếu đã có tới hơn 74.000 cảnh báo tấn công mạng.

Năm 2025 sẽ tiếp tục chứng kiến sự bùng nổ của các công nghệ mới như trí tuệ nhân tạo (AI), công nghệ chuỗi khối (blockchain), điện toán lượng tử. Các mã độc sẽ có khả năng tự nâng cấp, công nghệ Deepfake được cải tiến và các công cụ AI tạo sinh khác sẽ giúp kẻ xấu tạo nội dung giả mạo khó lường hơn. Điện toán lượng tử, dù còn ở giai đoạn sơ khai, nhưng cũng có khả năng phá vỡ các thuật toán mã hóa truyền thống, gây lo ngại lớn cho việc bảo vệ dữ liệu.

Hacker sẽ sử dụng AI để tự động hóa các cuộc tấn công. Công nghệ 5G phát triển sẽ kéo theo số lượng thiết bị IoT tăng mạnh, cùng với đó sẽ có nhiều lỗ hổng bảo mật trên các thiết bị này có thể bị khai thác, từ camera an ninh, đồng hồ thông minh đến thiết bị gia dụng.

Người dùng cá nhân cần trang bị kiến thức, sử dụng các công cụ bảo mật tiên tiến và cẩn trọng hơn trong việc chia sẻ thông tin trên không gian mạng. Các cơ quan chức năng và tổ chức an ninh mạng cần phối hợp để đối phó hiệu quả với các thách thức mới, bảo vệ một không gian mạng an toàn và đáng tin cậy hơn.

SỬ DỤNG AI, SEARCH….

- Dùng ChatGPT hoặc Google, DeepSeek,… hỏi:
  "Tình hình an ninh mạng hiện nay như thế nào" ➔
  Các em ghi vào vở tóm tắt và giải thích ?
- Các nguy cơ mất an ninh mạng là gì?
- Tại sao an ninh mạng ngày càng quan trọng ?
- Thiệt hại từ mất an ninh mạng như thế nào?

CÁC HÌNH THỨC MẤT AN TOÀN

LỪA ĐẢO QUA EMAIL

QUY TRÌNH LỪA ĐẢO TỐNG TIỀN QUA EMAIL VÀ CÁCH PHÒNG TRÁNH

BƯỚC 1

Gửi thư giả mạo tống tiền cho người dùng

BƯỚC 3

Người dùng nhẹ dạ, cả tin và thực hiện sẽ bị mất tài sản

BƯỚC 2

Nội dung tống tiền bao gồm :

Thông báo email lộ mật khẩu
Đã cài đặt virus vào thiết bị
Yêu cầu chuyển tiền tài khoản đã cung cấp
Có dữ liệu video nhạy cảm của người dùng
Không thực hiện sẽ phát tán thông tin cá nhân

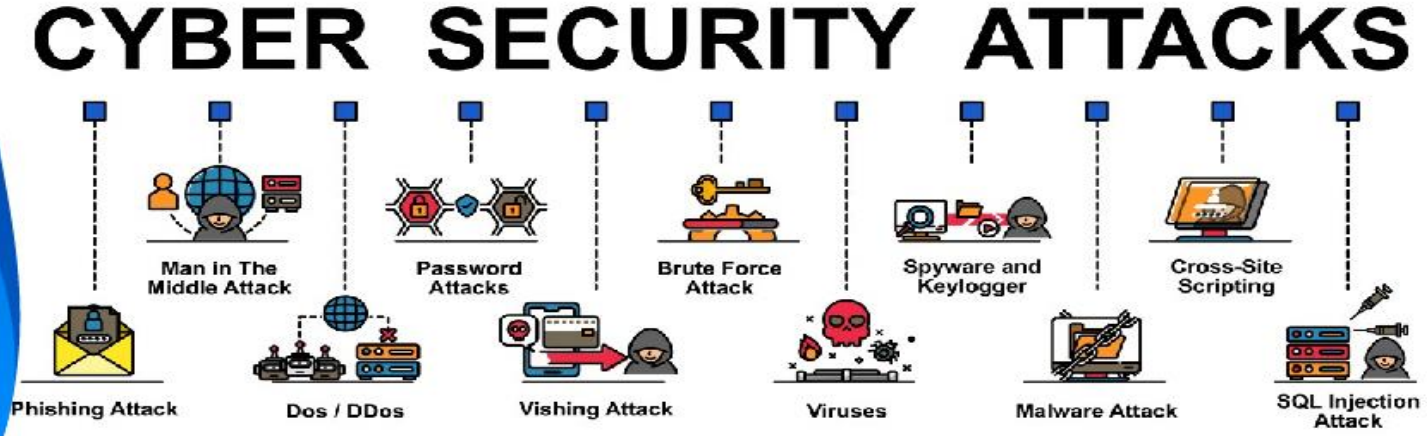
Hình thức mất an toàn mạng

- Phần mềm độc hại (Malware): Phần mềm độc hại bao gồm virus, worm, trojan, ransomware, spyware và adware
- DDoS Attack: Kẻ tấn công sử dụng nhiều máy tính bị lây nhiễm để gửi lượng lớn yêu cầu đến một máy chủ hoặc hệ thống, làm cho nó quá tải và không thể hoạt động bình thường.
- Phishing: Phishing là hành vi lừa đảo qua email hoặc trang web giả mạo nhằm đánh cắp thông tin cá nhân, thông tin đăng nhập, hoặc dữ liệu tài chính của người dùng.

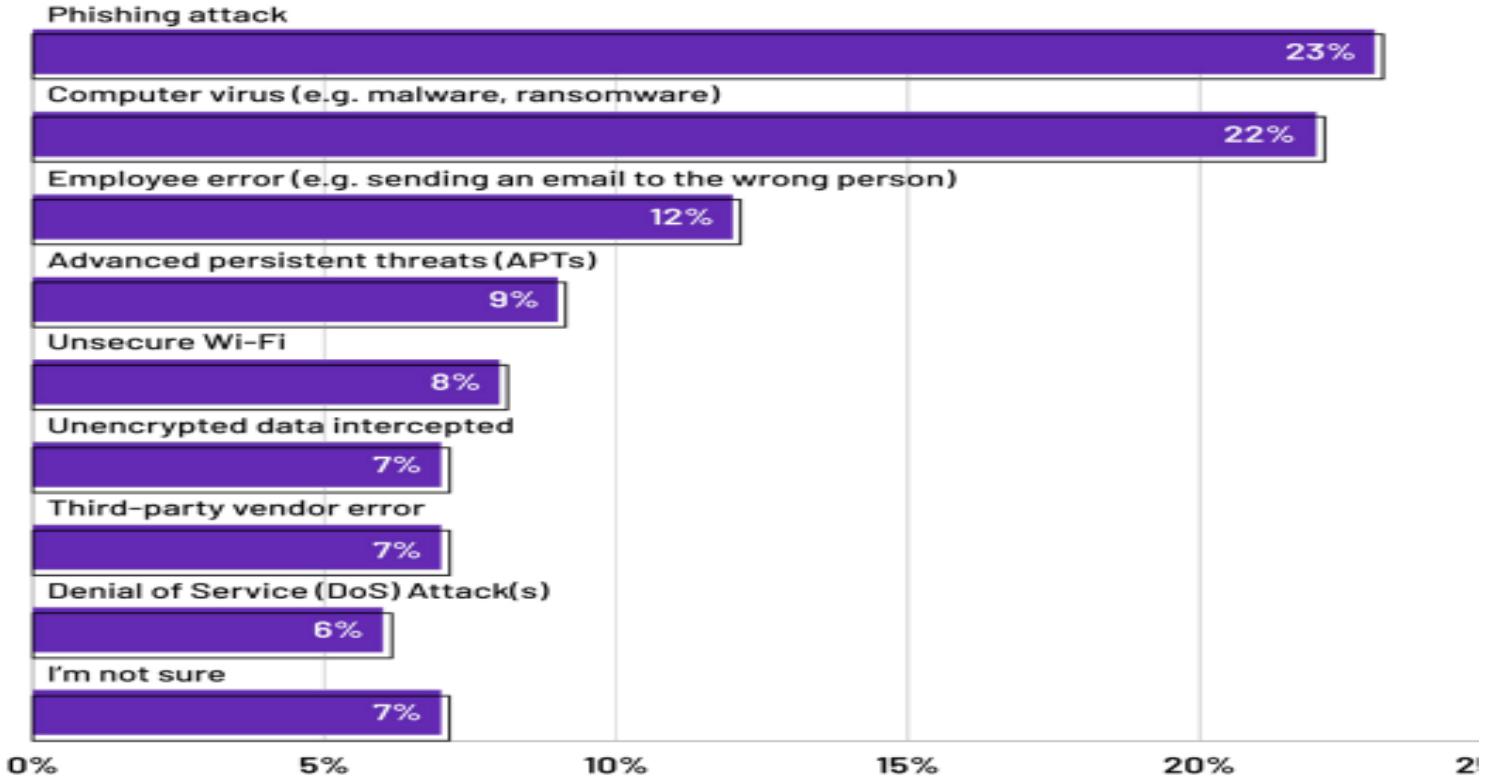
Hình thức mất an toàn mạng

- Tấn công khai thác lỗ hổng: Kẻ tấn công có thể tận dụng các lỗ hổng bảo mật trong phần mềm, hệ điều hành, hoặc ứng dụng để xâm nhập vào hệ thống, chiếm quyền kiểm soát hoặc đánh cắp dữ liệu.
- Tấn công qua mạng xã hội: Tấn công qua mạng xã hội là hình thức tấn công mà kẻ tấn công thao túng tâm lý con người để lừa họ tiết lộ thông tin mật hoặc thực hiện các hành động không an toàn.
- Tấn công mã hóa tống tiền (Ransomware): Ransomware là một loại malware mã hóa các tệp dữ liệu quan trọng trên máy tính hoặc hệ thống mạng và yêu cầu một khoản tiền chuộc để giải mã chúng.

Hình thức mất an toàn mạng



DÙNG CHATGPT, GOOGLE, AI TÌM HIỂU?



Hình thức mất an toàn mạng sau là gì ?

The significance of the field stems from the expanded reliance on computer systems, the Internet, and wireless network standards. Its importance is further amplified by the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity has emerged as one of the most significant new challenges facing the contemporary world, due to both the complexity of information systems and the societies they support. Security is particularly crucial for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

Các loại hình tấn công mạng

- Malware – Tấn công bằng phần mềm độc hại
- Tấn công giả mạo (Phishing)
- Tấn công từ chối dịch vụ (Dos và DDoS)
- Tấn công trung gian (Man-in-the-middle attack)
- Khai thác lỗ hổng Zero-day (Zero day attack)

Tấn công Malware

Tấn công Malware là gì?

Tấn công Malware

- Spyware (phần mềm gián điệp)
- Ransomware (mã độc tống tiền)
- Virus
- Worm (phần mềm độc hại lây lan với tốc độ nhanh)

Tấn công Malware

- Hacker sẽ tiến hành tấn công người dùng thông qua các lỗ hổng bảo mật.
- Lừa người dùng Click vào một đường Link hoặc Email để cài phần mềm độc hại tự động vào máy tính.

Tấn công Malware

Malware sẽ gây ra những hậu quả nghiêm trọng:

- Chặn các truy cập vào hệ thống mạng và dữ liệu quan trọng (Ransomware).
- Cài đặt thêm phần mềm độc hại khác vào máy tính người dùng.
- Đánh cắp dữ liệu (Spyware).
- Phá hoại phần cứng, phần mềm, làm hệ thống bị tê liệt, không thể hoạt động.

Cách phòng chống Malware

- **Sao lưu dữ liệu thường xuyên:** Việc này sẽ giúp chúng ta không phải lo lắng khi dữ liệu bị phá hủy.
- **Thường xuyên cập nhật phần mềm:** Các bản cập nhật của phần mềm (trình duyệt, hệ điều hành, phần mềm diệt Virus,…) sẽ vá lỗi bảo mật còn tồn tại trên phiên bản cũ, đảm bảo an toàn thông tin cho người dùng.
- **Cẩn thận với các Link hoặc File lạ:** Đây là phương thức lừa đảo khá phổ biến của Hacker. Chúng sẽ gửi Email hoặc nhắn tin qua Facebook, đính kèm Link Download và nói rằng đó là File quan trọng hoặc chứa nội dung hấp dẫn.
- Khi tải về, các File này thường nằm ở dạng .docx, .xlxs, .pptx hay .pdf, nhưng thực chất là File .exe (chương trình có thể chạy được). Ngay lúc người dùng Click mở File, mã độc sẽ lập tức bắt đầu hoạt động.

Tấn công giả mạo (Phishing)

Tấn công Phishing là gì?

Tấn công giả mạo (Phishing)

- **Phishing (tấn công giả mạo)** là hình thức tấn công mạng bằng giả mạo thành một đơn vị uy tín để chiếm lòng tin và yêu cầu người dùng cung cấp thông tin cá nhân cho chúng.
- Hacker sẽ 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 như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quan trọng khác.

Phishing

- Phương thức tấn công này thường được thực hiện thông qua việc gửi Email và tin nhắn. Người dùng khi mở Email và Click vào đường Link giả mạo sẽ được yêu cầu đăng nhập ➔ tin tặc sẽ có được thông tin cá nhân.
- Thuật ngữ là sự kết hợp của 2 từ: Fishing For Information (câu thông tin) và Phreaking (trò lừa đảo sử dụng điện thoại của người khác không trả phí).

Các phương thức tấn công Phishing

Giả mạo Email:

- Đây là hình thức Phishing khá căn bản. Tin tặc sẽ gửi Email đến người dùng dưới danh nghĩa của một đơn vị/tổ chức uy tín nhằm dẫn dụ người dùng truy cập đến Website giả mạo
- Những Email giả mạo thường rất tinh vi và rất giống với Email chính chủ, khiến người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công.

Tấn công Phishing

Giả mạo Website

- Giả mạo Website trong tấn công Phishing là làm giả một trang chứ không phải toàn bộ Website. Trang được làm giả thường là trang đăng nhập để cướp thông tin của người dùng.
- Website giả thường có những đặc điểm sau:
- Thiết kế giống đến 99% so với Website gốc.
- Đường dẫn chỉ khác 1 ký tự duy nhất
  (VD: **facebook.com** và **fakebook.com**, **microsoft.com** và **mircosoft.com**,…)
- Luôn có những thông điệp khuyến khích người dùng cung cấp thông tin cá nhân.

Chống tấn công Phishing

Cách phòng chống tấn công Phishing

- Cảnh giác với các Email có xu hướng thúc giục chúng ta nhập thông tin cá nhân, thông tin nhạy cảm (thông tin thẻ tín dụng, thông tin tài khoản,..)
- Không Click vào các đường dẫn được gửi đến Email nếu không chắc chắn an toàn.
- Không trả lời những thư rác, lừa đảo.
- Luôn cập nhật phần mềm, ứng dụng đề phòng các lỗ hổng bảo mật có thể bị tấn công.

Công cụ hạn chế Phishing

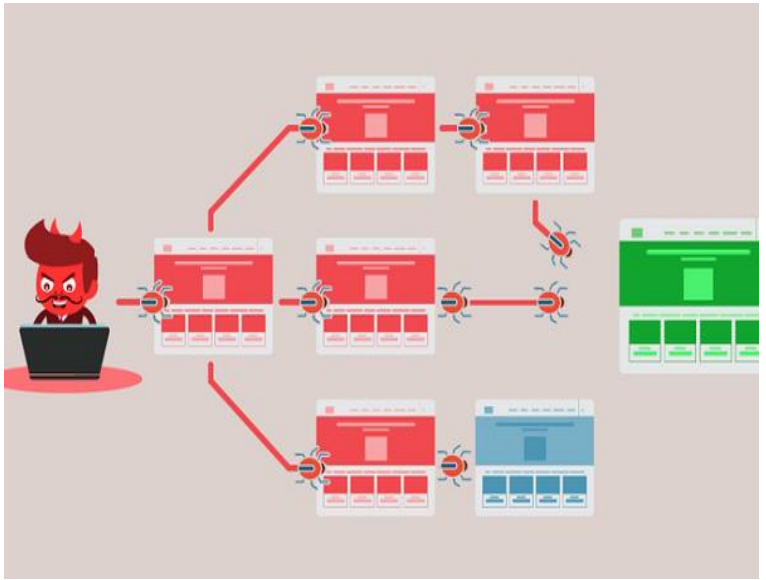
- **SpoofGuard:** Đây là một Plugin trình duyệt tương thích với Microsoft Internet Explorer. SpoofGuard sẽ đặt “cảnh báo” trên thanh công cụ của trình duyệt. Nó sẽ chuyển từ màu xanh sang màu đỏ nếu chúng ta vô tình truy cập vào Website giả mạo Phishing. Nếu chúng ta cố nhập các thông tin quan trọng vào một trang giả mạo, SpoofGuard sẽ lưu dữ liệu của chúng ta và đưa ra cảnh báo.
- **Anti-phishing Domain Advisor**: Thực chất đây là một Toolbar (thanh công cụ) giúp cảnh báo những trang web lừa đảo, dựa theo dữ liệu của công ty Panda Security.
- **Netcraft Anti-phishing Extension**: Netcraft là đơn vị uy tín trong việc cung cấp các dịch vụ bảo mật. Trong số đó, tiện ích mở rộng chống Phishing của Netcraft được đánh giá rất tốt với nhiều tính năng cảnh báo thông minh cho người dùng.

Tấn công DoS

Các em hiểu tấn công DoS là gì ?

Tấn công DoS

- **DoS (Denial of Service)** là "đánh sập tạm thời" một hệ thống, máy chủ hoặc mạng nội bộ.
- Hacker thường tạo ra một lượng Traffic/Request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải.
- Người dùng sẽ không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

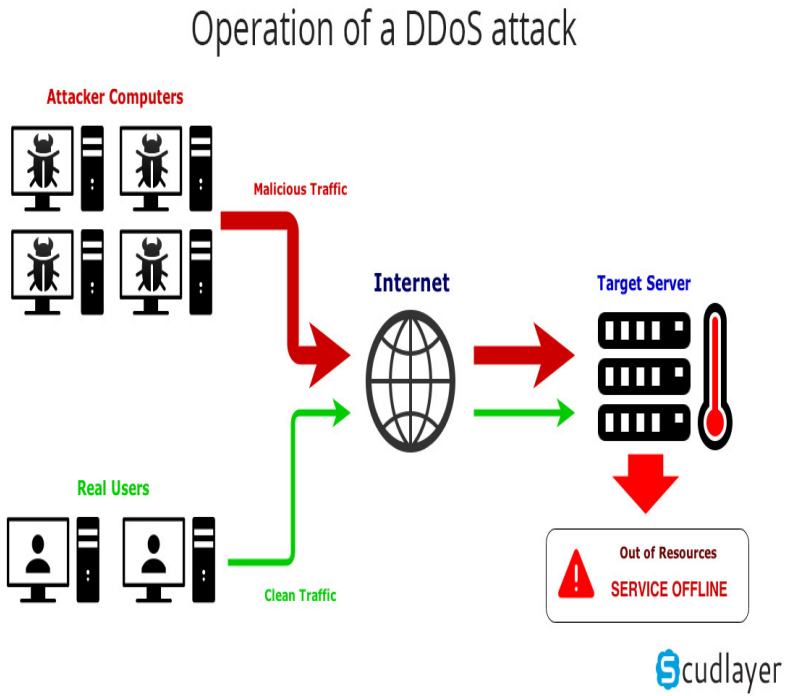


Tấn công DoS

- Nạn nhân của tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội...
- Ví dụ, khi chúng ta nhập vào URL của một website vào trình duyệt, lúc đó chúng ta đang gửi một yêu cầu đến máy chủ của trang này để xem.
- Máy chủ chỉ có thể xử lý một số yêu cầu nhất định trong một khoảng thời gian, vì vậy nếu kẻ tấn công gửi ồ ạt nhiều yêu cầu đến máy chủ sẽ làm nó bị quá tải và yêu cầu của chúng ta không được xử lý. Đây là kiểu "từ chối dịch vụ" vì nó làm cho chúng ta không thể truy cập đến trang đó.

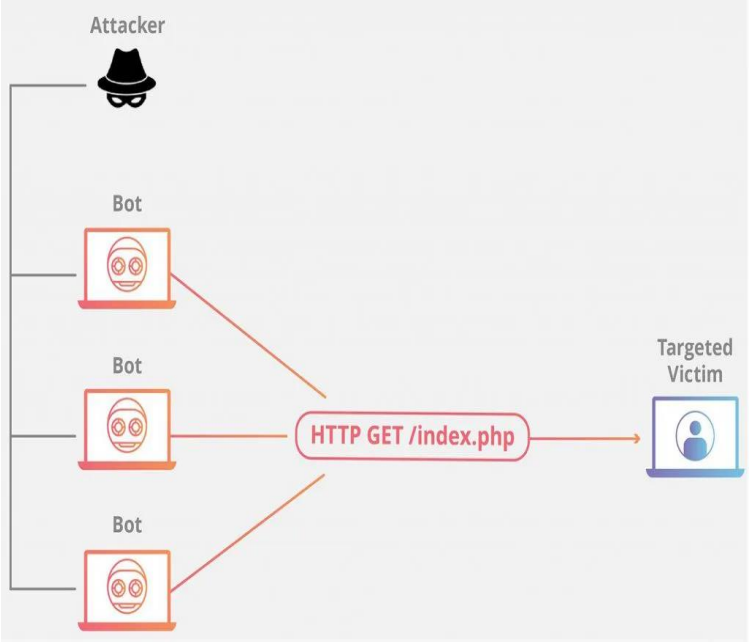
Tấn công DDoS

Các em hiểu tấn công DDoS là gì ?



Tấn công DDoS

- **DDoS (Distributed Denial of Service)**: Tin tặc sử dụng một mạng lưới các máy tính (Botnet) để tấn công người dùng, vấn đề ở đây là chính các máy tính thuộc mạng lưới Botnet sẽ không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.
- DDoS (Distributed Denial of Service), nghĩa tiếng Việt là từ chối dịch vụ phân tán.
- Tấn công DDoS là nỗ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập nó với traffic từ nhiều nguồn.



Tấn công DDoS

- Khi DDoS, kẻ tấn công có thể sử dụng máy tính của chúng ta để tấn công vào các máy tính khác.
- Bằng cách lợi dụng những lỗ hổng về bảo mật cũng như sự không hiểu biết, kẻ này có thể giành quyền điều khiển máy tính của chúng ta.
- Sau đó chúng sử dụng máy tính của chúng ta để gửi số lượng lớn dữ liệu đến một website hoặc gửi thư rác đến địa chỉ email nào đó.
- Đây là kiểu tấn công phân tán vì kẻ tấn công sử dụng nhiều máy tính, bao gồm có cả máy tính của chúng ta để thực hiện tấn công Dos.

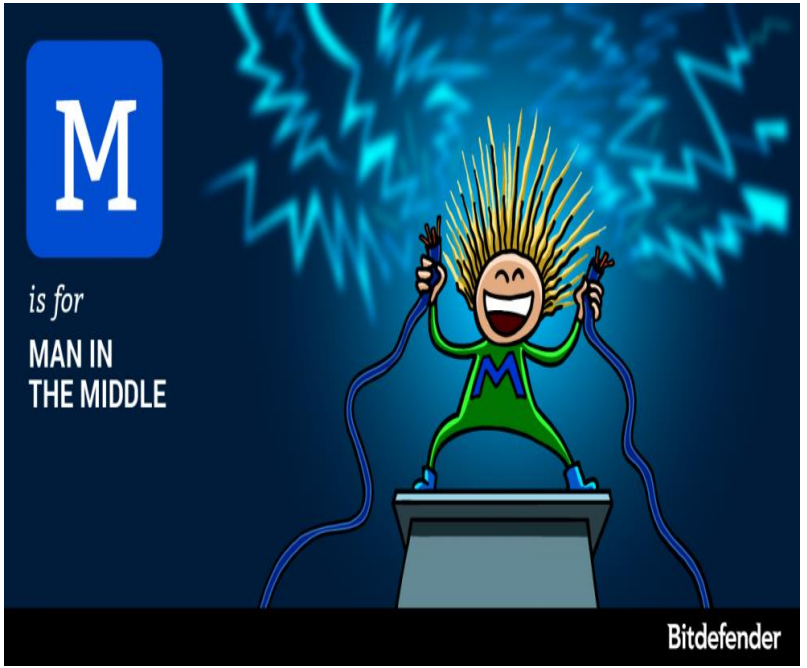
Tấn công DDoS

Mặc dù DDoS cung cấp một chế độ tấn công ít phức tạp hơn các dạng tấn công mạng khác, nhưng chúng đang ngày càng mạnh mẽ và tinh vi hơn. Có ba loại tấn công cơ bản:

- **Volume-based:** Sử dụng lưu lượng truy cập cao để làm tràn ngập băng thông mạng
- **Protocol:** Tập trung vào việc khai thác các tài nguyên máy chủ
- **Application:** Tập trung vào các ứng dụng web và được xem là loại tấn công tinh vi và nghiêm trọng nhất

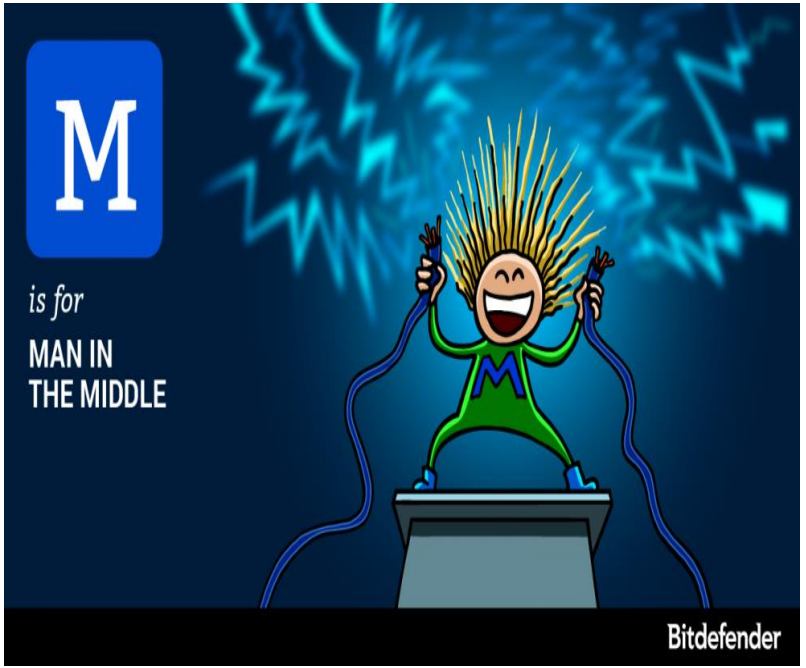
Man-in-the-middle attack

Tấn công trung gian (Man-in-the-middle attack) là gì ?



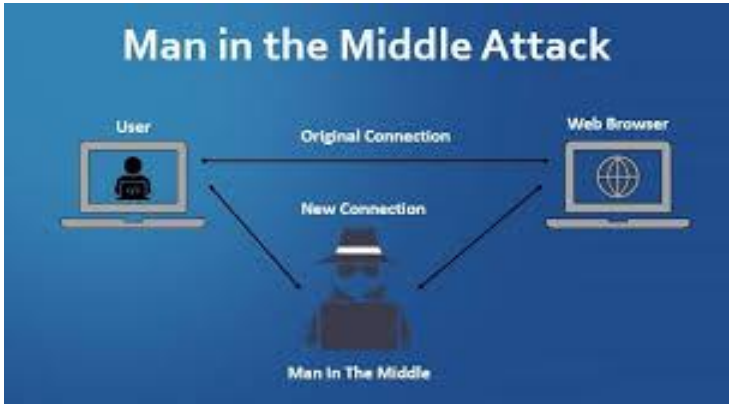
Tấn công trung gian

- Một cuộc tấn công MitM thường là một cuộc tấn công linh hoạt, xâm chiếm và bí mật.
- Tấn công man-in-the-middle xảy ra khi ai đó ở giữa hai máy tính (máy tính xách tay và máy chủ từ xa) và có khả năng chặn lưu lượng truy cập.
- Kẻ đó có thể nghe trộm hoặc thậm chí chặn liên lạc giữa hai máy và đánh cắp thông tin nhạy cảm.



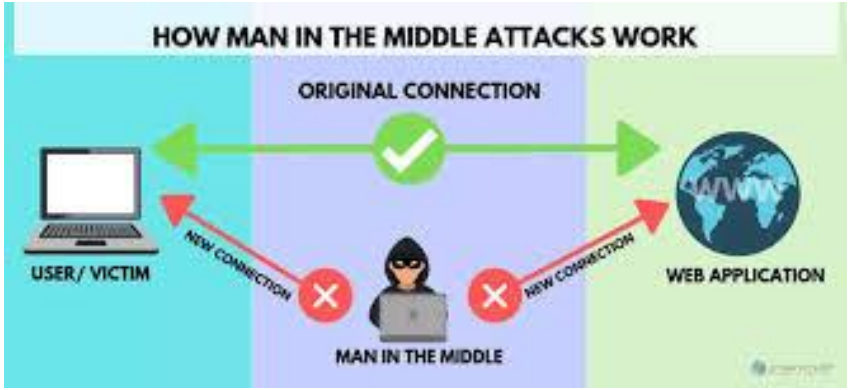
Hình thức tấn công trung gian

- **Sniffing**: Sniffing hoặc Packet Sniffing là kỹ thuật được sử dụng để nắm bắt các gói dữ liệu vào và ra của hệ thống.
- **Packet Injection**: Kẻ tấn công sẽ đưa các gói dữ liệu độc hại vào với dữ liệu thông thường mà người dùng không nhận thấy tệp/phần mềm độc hại bởi chúng đến như một phần của luồng truyền thông hợp pháp.



Hình thức tấn công trung gian

- **Gỡ rối phiên**: Khoảng thời gian từ lúc đăng nhập vào tài khoản ngân hàng đến khi đăng xuất khỏi tài khoản đó được gọi là một phiên. Một Hacker thiết lập sự hiện diện của mình trong phiên và kiểm soát nó.
- **Loại bỏ SSL**: SSL Stripping hoặc SSL Downgrade Attack là các cuộc tấn công MiTM. Kẻ tấn công loại bỏ kết nối SSL/TLS và chuyển giao thức từ HTTPS an toàn sang HTTP không an toàn.



Cách phòng chống tấn công trung gian

- Đảm bảo các Website chúng ta truy cập đã cài SSL.
- Không mua hàng hoặc gửi dữ liệu nhạy cảm khi dùng mạng công cộng.
- Không nhấp vào Link hoặc Email độc hại.
- Có các công cụ bảo mật thích hợp được cài đặt trên hệ thống của chúng ta.
- Tăng cường bảo mật cho hệ thống mạng của gia đình chúng ta.

ĐẠI NAM UNIVERSITY

Thế nào là tấn công khai thác lỗ hổng Zero-day (Zero day attack) ???

Khai thác lỗ hổng Zero-day (Zero day attack)

- **Lỗ hổng zero-day (0-day Vulnerability)** thực chất là những lỗ hổng bảo mật của phần mềm hoặc phần cứng mà người dùng chưa phát hiện ra.
- Tồn tại trong nhiều môi trường khác nhau như: Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm – phần cứng máy tính, thiết bị IoT, Cloud, …

Khai thác lỗ hổng Zero-day (Zero day attack)

- **Lỗ hổng zero-day (0-day Vulnerability)** thực chất là những lỗ hổng bảo mật của phần mềm hoặc phần cứng mà người dùng chưa phát hiện ra.
- Tồn tại trong nhiều môi trường khác nhau như: Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm – phần cứng máy tính, thiết bị IoT, Cloud, …

Khai thác lỗ hổng Zero-day (Zero day attack)

- Lỗ hổng Zero-day là những lỗ hổng chưa được biết tới bởi đối tượng sở hữu hoặc cung cấp sản phẩm chứa lỗ hổng.
- Bản vá bảo mật cho lỗ hổng này để người dùng được bảo mật tốt hơn.
- Một khi được công bố rộng rãi ra công chúng, lỗ hổng 0-day trở thành lỗ hổng n-day.

Cách phòng chống lỗ hổng Zero-day

- Thường xuyên cập nhật phần mềm và hệ điều hành
- Triển khai giám sát bảo mật theo thời gian thực
- Triển khai hệ thống IDS và IPS
- Sử dụng phần mềm quét lỗ hổng bảo mật

ĐẠI NAM UNIVERSITY

Các loại hình tấn công khác ???

Các loại hình tấn công khác

Ngoài ra, còn rất nhiều **hình thức tấn công mạng** khác như:

- Tấn công chuỗi cung ứng
- Tấn công Email
- Tấn công vào con người
- Tấn công nội bộ tổ chức

GIẢI PHÁP BẢO ĐẢM AN TOÀN

Các giải pháp thực hiện

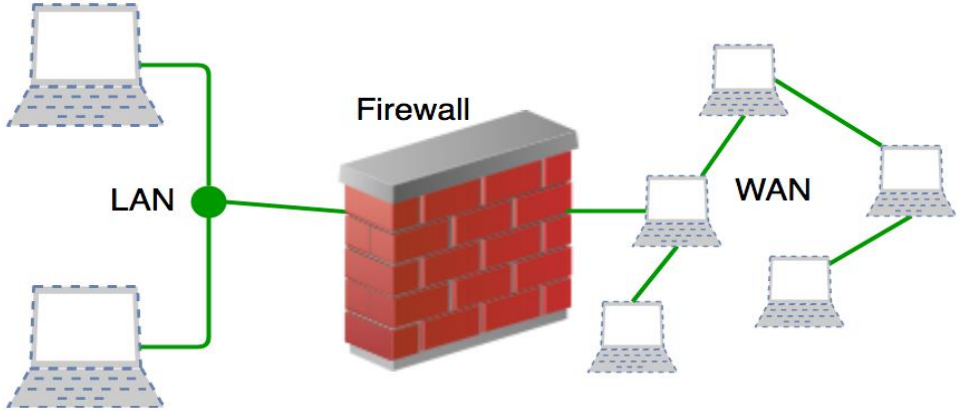
1. Sử dụng Tường lửa
2. Chia nhỏ mạng nội bộ
3. Phát hành chính sách an ninh mạng
4. Hướng dẫn cho toàn bộ nhân viên
5. Áp dụng mật khẩu an toàn
6. Thường xuyên sao lưu dữ liệu

7. Cài đặt phần mềm chống mã độc
8. Sử dụng xác thực đa yếu tố
9. Luôn cảnh giác
10. Mã hóa và phân chia dữ liệu khách hàng
11. Luôn thận trọng với phần mềm miễn phí
12. Tăng bảo mật email

GIẢI PHÁP ĐẢM BẢO AN TOÀN MẠNG

- **Dùng ChatGPT hỏi:**

1. **Bức tường lửa (firewall) là gì?**



Xem video (3 phút):
https://www.youtube.com/watch?v=uT_xe4YNI_g

➔ Các em phát biểu tóm tắt lại: Tường lửa là gì? SV sẽ được cộng điểm.

If an attacker gains access to your company's network, one of your main goals should be to limit the amount of damage they may cause. Another goal should be to slow down the attacker as much as possible until you can cut them off.

A firewall is considered the foundation of cybersecurity solutions since it helps to stop or slow down an attack. It is the most crucial tool your company could have. A firewall keeps an eye on network traffic or attempts to connect and blocks those that could hurt your website or web application.

Cybercriminals with advanced skills have discovered ways to produce data or software that bypasses firewalls and gets access. But you can deal with this by using network scanners, which give your network more security against SQL injection, illegal resource access, cross-site scripting, and other OWASP (Open Web Application Security) threats.

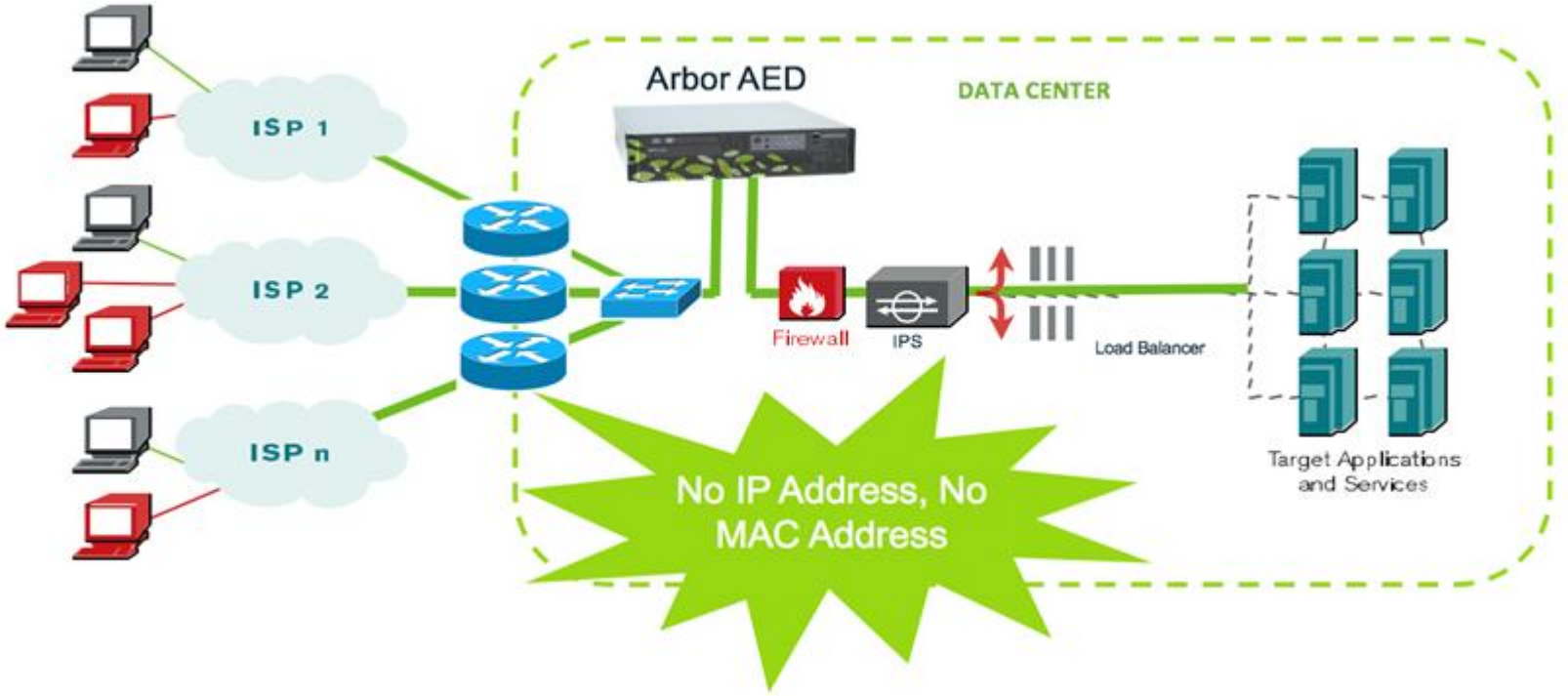
THIẾT LẬP MẬT KHẨU MẠNH

Theo các em, đặt mật khẩu mạnh nên như thế nào ?

GIẢI PHÁP ĐẢM BẢO AN TOÀN MẠNG

- Xây dựng kế hoạch **sao lưu, phục hồi dữ liệu** đối với hệ thống, thông tin quan trọng.
- Triển khai các biện pháp **xác thực mạnh** cho các tài khoản truy cập hệ thống.
- Chủ động tìm kiếm dấu hiệu tấn công, rà quét mã độc, yêu cầu đơn vị chuyên trách xử lý các mã độc.
- Giám sát liên tục để phát hiện sớm các hành vi xâm nhập, đặc biệt giám sát các truy cập đến **vCenter, ESXI, Domain Control-**
- **Rà quét, cập nhật** bản vá lỗ hổng an toàn thông tin trên các thiết bị, phần mềm, ứng dụng.
- **Xây dựng kế hoạch** ứng phó sự cố để kịp thời phản ứng với sự cố Ransomware.
- Áp dụng các **nguyên tắc đặc quyền** tối thiểu cho các hệ thống.
- **Hạn chế** việc sử dụng **dịch vụ** điều khiển máy tính **từ xa**.
- Thực hiện **phân vùng** mạng chặt chẽ.

CHỐNG TẤN CÔNG DDOS



Đo lưu lượng mạng, phát hiện tấn công và giảm thiểu các cuộc tấn công

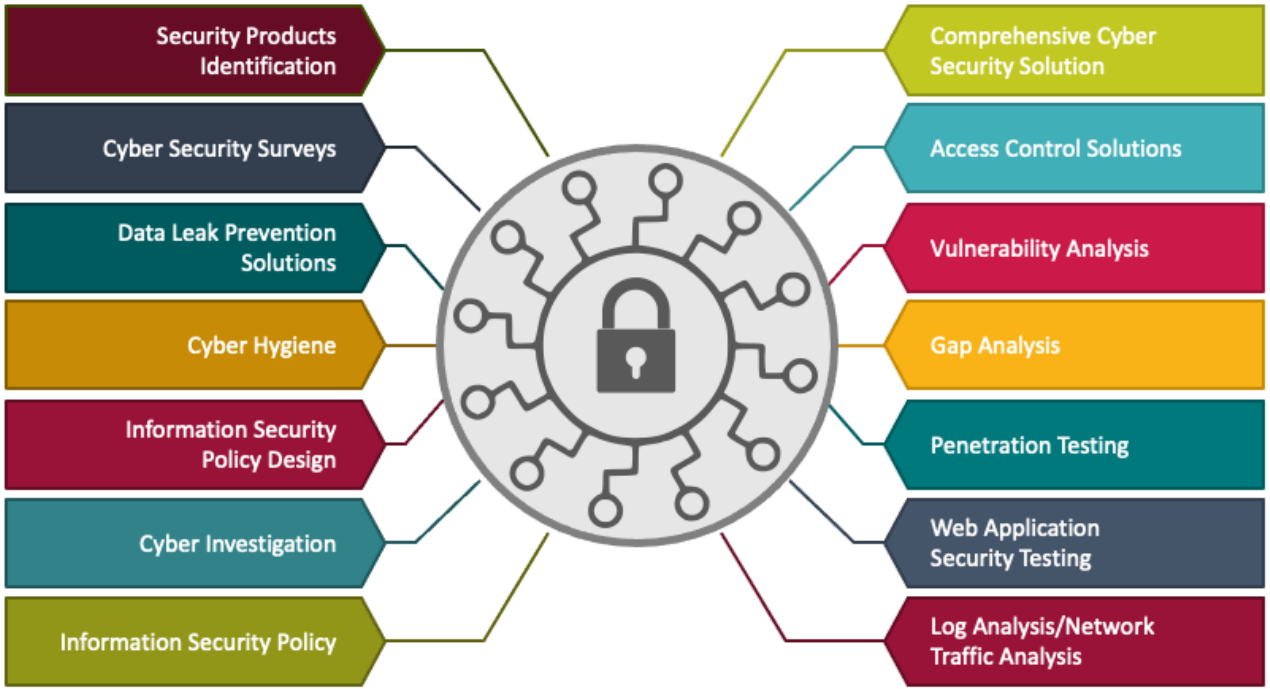
Các giải pháp thực hiện

Các giải pháp thực hiện

Các giải pháp thực hiện

Các giải pháp thực hiện

CYBERSECURITY SOLUTIONS



With hackers and cybercriminals growing more sophisticated (including the technology and software they use), businesses must invest more in cyber defence and security.

The first step in becoming cyber secure is to assess and comprehend the current gaps in your company's security. You may do an evaluation to see how vulnerable you are.

Instead of waiting for a cyberattack on your IT infrastructure and dealing with the fallout, it is better to find and fix vulnerabilities in your system before they happen.

SUMMARY

- Khái niệm an ninh mạng
- Các hình thức mất an ninh mạng
- Giải pháp đảm bảo an ninh mạng

ĐẠI NAM
UNIVERSITY