NETPRO ACADEMY
Your training partner to success

Giảng viên: Ths. Hồ Kim Cường

Email: cuonghk@vncert.vn

Di động: 0904 361 245

https://www.facebook.com/hocuong24

CEI Certified EC-Council Instructor

CHFI Computer Hacking Forensic INVESTIGATOR

ECSA EC-Council Certified Security Analyst

CEH Certified Ethical Hacker

Linux Professional Institute LPIC-1

Linux Professional Institute LPIC-2

NETPRO ACADEMY
Your training partner to success

KHÓA HỌC

AN TOÀN THÔNG TIN CHO NGƯỜI DÙNG VÀ CÁN BỘ KỸ THUẬT

Nội dung của khóa học

1. Tổng quan về an toàn thông tin
2. Các nguy cơ tấn công người dùng và hệ thống thông tin của tổ chức
3. Các biện pháp bảo đảm an toàn thông tin cho người dùng và tổ chức
4. **Các kỹ thuật tấn công nâng cao của tin tặc**
5. **Phân tích, bóc gỡ mã độc**
6. **Phát hiện và ngăn chặn tấn công mạng và ứng phó sự cố**

NETPRO ACADEMY
Your training partner to success

TỔNG QUAN VỀ AN TOÀN, AN NINH THÔNG TIN

- Cập nhật tình hình an toàn thông tin ở VN và trên TG
- Khái niệm về Chính phủ điện tử, Chính phủ số, Kinh tế số, xã hội số
- Các khái niệm về ATTT: tính bí mật, sẵn sàng, toàn vẹn, rủi ro, lỗ hổng bảo mật, mối đe dọa,

Tình hình an toàn thông tin

TẠI VIỆT NAM

TRÊN THẾ GIỚI

Tình hình ATTT trên thế giới (1)

- Thế kỷ phụ thuộc vào công nghệ thông tin

Tính toàn cầu (Bạn ở khắp mọi nơi)

Dễ dàng kết bạn không khoảng cách

Tìm kiếm khách hàng mới

Tìm kiếm các cơ hội mới

Khả năng giao tiếp (ngay tức thời)

Text messaging

Social media

Emails

Video streaming

Kinh doanh trực tuyến

Dễ dàng giới thiệu sản phẩm đến nhiều đối tượng.

Giảm chi phí nhưng tăng lợi nhuận

Chính phủ điện tử

Một số mạng xã hội phổ biến tại Việt Nam

Mục đích sử dụng MXH tại Việt Nam

Tình hình ATTT trên thế giới (cont')

- Thế giới kiểu "Bring Your Own Device" ("BYOD")
- Các thiết bị di động trở thành mục tiêu tấn công phổ biến.
- Cài cắm mã độc và tấn công doanh nghiệp
- Các tin tặc được chính phủ tài trợ nhằm do thám và phá hoại các cơ sở hạ tầng quan trọng

Không ai an toàn 100% chỉ là khi nào sẽ bị tấn công và thường xuyên không

Tình hình ATTT trên thế giới (cont')

- Ngày 10/3/2021. Tờ báo Newsweek.com đăng tin. Quân đội Mỹ gửi các cảnh báo tới Trung Quốc về việc nước này sử dụng 1 triệu người làm "cỗ máy tin giả" nhằm phá hoại các giá trị của nền dân chủ Mỹ cũng như các nền dân chủ khác.

- Hành động được cho là nhằm chia cắt sợi dây liên kết giữa Mỹ với các nước châu Á và xây dựng quyền bá chủ của mình tại đây.

https://www.newsweek.com/chinas-1-million-strong-disinformation-machine-eroding-us-hegemony-admiral-1575057?utm_source=Flipboard&utm_medium=App&utm_campaign=Partnerships

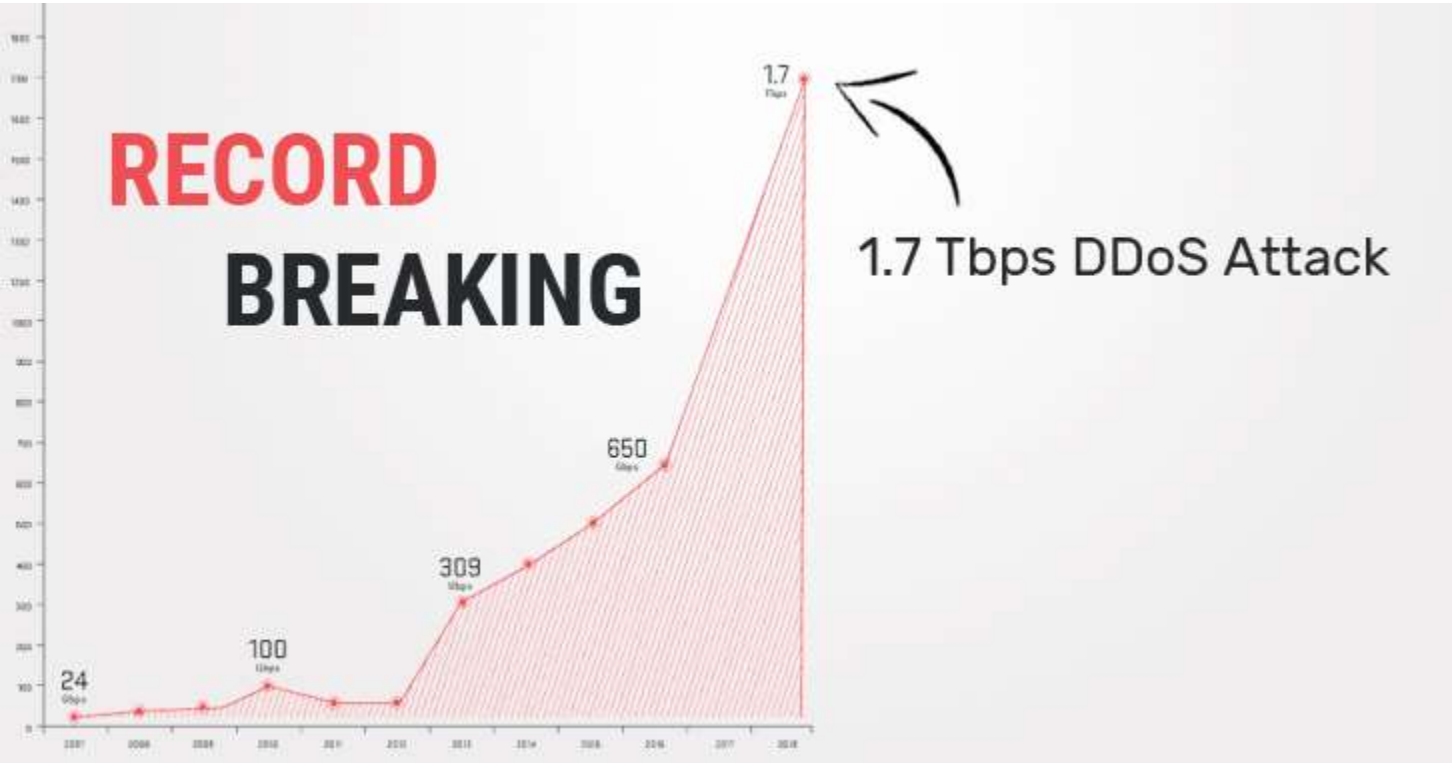
Tình hình ATTT trên thế giới (cont')

Các chuyên gia bảo mật Mỹ và Anh đã phát hiện, vào cuối năm 2019 tin tặc Nga đã đánh cắp nội dung thỏa thuận thương mại bí mật giữa Mỹ và Anh qua tài khoản email của cựu bộ trưởng nội các Liam Fox! Chính phủ Anh tuyên bố đã tìm thấy các nhóm Nga chịu trách nhiệm quảng bá các tài liệu này và một cuộc điều tra hình sự đã được mở.

https://news.sky.com/story/russian-hackers-stole-us-uk-trade-talk-papers-from-email-account-of-liam-fox-report-12041778

Tình hình ATTT trên thế giới (cont')

TẤN CÔNG DDoS LỚN NHẤT TRONG LỊCH SỬ



Tấn công Memcached DDoS xảy ra vào tháng 3/2018

Nguồn: https://thehackernews.com/2018/03/ddos-attack-memcached.html
https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

Tình hình ATTT tại Việt Nam (1)

- Ngày 05/4/2021, hãng bảo mật Kaspersky đã công bố thông tin về các hoạt động gián điệp mạng nhắm vào Chính phủ và Quân đội Việt Nam .
- Nhóm tin tặc Trung Quốc nhắm vào các cơ quan thuộc Chính phủ như Bộ Ngoại giao, Công an, Nội vụ, Tài chính, Kế hoạch - Đầu tư, Văn phòng Chính phủ,.. trong khoảng thời gian từ tháng 6/2020 đến tháng 01/2021.
- Theo Kaspersky, nhóm tin tặc có nguồn gốc Trung Quốc có tên là Cycldek (còn được biết tên với các tên gọi “Goblin Panda” và Conimes) bắt đầu hoạt động từ năm 2013 chuyên tấn công vào các Chính phủ khu vực Đông Nam Á.

Tình hình ATTT tại Việt Nam (cont)

- Tấn công Vietnamairlines ngày 29/7/2016

Tình hình ATTT tại Việt Nam (cont)

The 10 Worst Botnet Countries

As of 04 October 2019 the world's worst botnet infected countries are:

1	India	Number of Bots: 2745390
2	China	Number of Bots: 1542893
3	Iran (Islamic Republic of)	Number of Bots: 1056660
4	Egypt	Number of Bots: 1025534
5	Viet Nam	Number of Bots: 966489

Nguồn: https://www.spamhaus.org/statistics/botnet-cc/

1.2. Một số khái niệm về ATTT (1)

An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ (Confidentiallity), gián đoạn (Availability), sửa đổi (Intergrity) hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin (Luật ATTT)

Nói cách khác, đảm bảo an toàn thông tin là đảm bảo ba thuộc tính sau:

- Tính bí mật (Confidentiallity)
- Tính toàn vẹn (Intergrity)
- Tính sẵn sàng (Availability)

1.2. Một số khái niệm về ATTT (1)

- Tính bí mật (Confidentiality): Là đảm bảo thông tin chỉ được truy xuất bởi những đối tượng được cấp quyền.
- Tính toàn vẹn (Integrity): Là duy trì và đảm bảo tính chính xác và nhất quán của dữ liệu trên toàn bộ vòng đời của nó.
- Tính sẵn sàng (Availability): Thông tin phải sẵn có khi cần thiết, không bị gián đoạn đối với đối tượng có quyền truy xuất.

- An ninh mạng: là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. (Luật ANM)

1.2. Một số khái niệm về ATTT (1)

Lỗ hổng bảo mật (vulnerable): Là điểm yếu của phần mềm hay của hệ thống thông tin, nó có thể bị khai thác bởi người dùng không hợp pháp hoặc bởi các tác nhân khác

Mối đe doạ (Threat): Là mối là tác nhân có thể khai thác lỗ hổng bảo mật để xâm phạm, gây thiệt hại cho hệ thống thông tin (làm ảnh hưởng đến thuốc tính C-I-A)

Rủi ro (Risk): Là khả năng (xác suất) một mối đe doạ tác động/gây hại đến tài sản thông tin bằng cách khai thác lỗ hổng bảo mật. Việc khai thác có thể tác động đến (Impact) các thuộc tính C-I-A

1.2. Một số ví dụ

Ví dụ về lỗ hổng bảo mật

- Người dùng, nhân viên kém nhận thức về ATTT
- Quy trình, chính sách thiếu, yếu, tuân thủ kém
- Các thành phần thiết bị công nghệ không được cập nhật, nâng cấp, rà soát lỗ hổng hoặc không được trang bị để bảo vệ theo nhiều lớp
- Thiếu các biện pháp kiểm soát vật lý, môi trường …

Ví dụ về mối đe dọa

- Lây nhiễm mã độc, hoặc các công cụ tấn công tinh vi
- Nhân viên vô tình hoặc cố ý trở thành mối đe dọa (kẻ tấn công),
- Attacker tấn công từ bên ngoài hoặc bên trong
- Trộm đột nhập đánh cắp tài sản thông tin
- Thiên tai, hỏa hoạn, động đất …

1.2. Một số ví dụ

(Bài tập: hãy cho biết đâu là ví dụ về vul/threat)

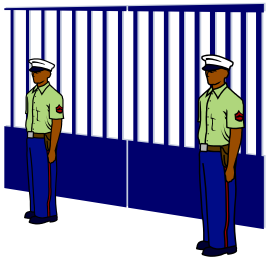
(1) Người dùng thiếu hiểu biết

(2) Trộm cắp. Phá hoại

(3) Malware

(4) Lỗi hệ thống

(5) Lack Of Documentation



(6) Mất cảnh giác trong việc bảo vệ phần vật lý

(7) Thảm hoạ thiên nhiên, cháy nổ

Thông tin xấu, độc trên mạng (1)

- Khoản 1 Điều 5 Nghị định 72/2013/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, ĐN thông tin xấu độc là:
  - Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam
  - Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc
  - Giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật
  - Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm
  - Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại
  - Tham khảo: https://thoidai.com.vn/the-nao-la-thong-tin-xau-doc-va-cac-muc-xu-ly-hanh-vi-dua-thong-tin-xau-doc-len-mang-127221.html

Thông tin xấu, độc trên mạng (2)

- Như vậy, thông tin xấu độc trên mạng internet là những thông tin dạng bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, "đổi trắng thay đen", làm lẫn lộn đúng sai, thật giả hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu sai trái, thù địch
- Xử lý các trường hợp đưa thông tin xấu, độc:
  - Phạt tiền 70 triệu đến 100 triệu (theo Khoản 6 Điều 66 Nghị định số 174/2013/NĐ-CP) => do tuyên truyền sai trái, không đúng sự thật về chủ quyền lãnh thổ quốc gia Việt Nam
  - Phạt tù đến 7 năm đối với (Điều 226 Bộ luật Hình sự năm 1999 sửa đổi năm 2009) Đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet; Phạt tù đến mức trung thân, nếu thực hiện hành vi chiếm đoạt tài sản (Điều 226b)

Nhu cầu cấp bách quản lý tin giả

Fake news (tin giả) đã được hãng từ điển Collins chọn là từ của năm 2017.
Từ này đã được sử dụng với tần suất chưa từng thấy, tăng 365% kể từ năm 2016.

Tin **GIẢ** lan nhanh gấp 6 lần tin **THẬT**

Mạng xã hội ngày càng có ảnh hưởng đến an ninh xã hội, chính trị

Tin tức lan nhanh do **những người có ảnh hưởng lớn, có nhiều người theo dõi**
Các ***bot*** tự động lan truyền thông tin xấu độc

Hiệu ứng đám đông, năng lực kiểm tra xác thực thông tin hạn chế

Các mạng xã hội nước ngoài chưa thiện chí hợp tác gỡ bỏ nội dung sai sự thật

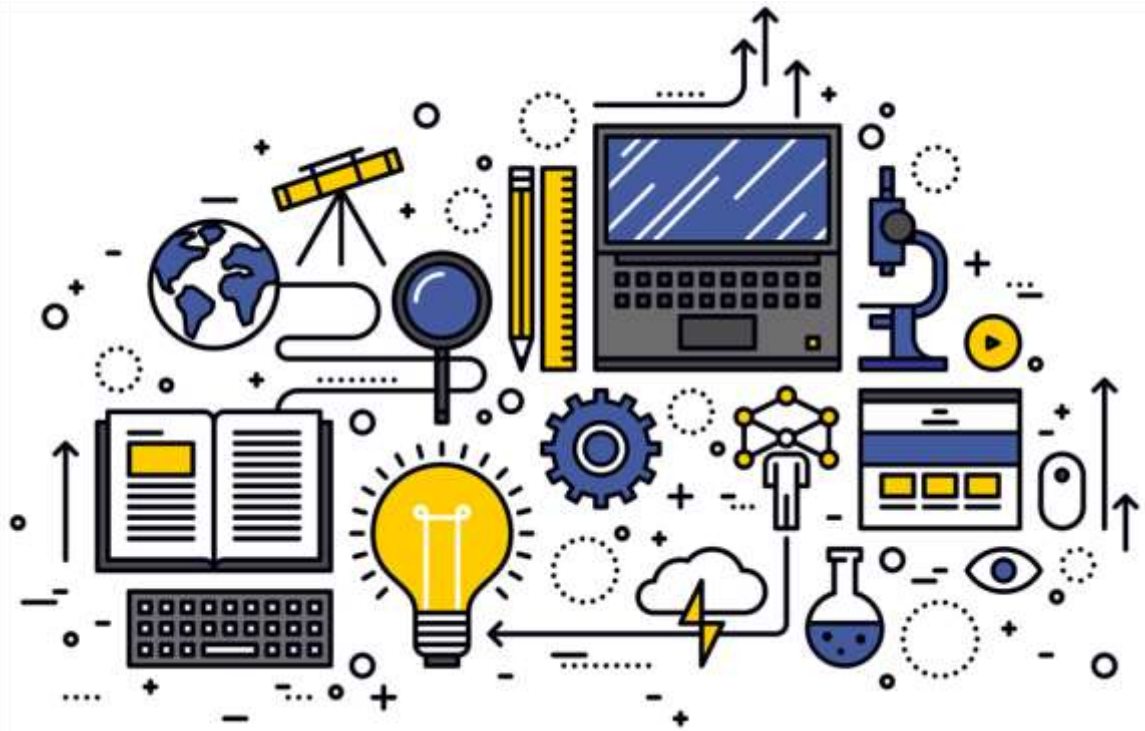
Các đối tượng đưa tin xấu độc

Tin học hóa là gì?

Tin học hóa hay còn gọi là ứng dụng công nghệ thông tin, là việc số hóa quy trình nghiệp vụ đã có. Thông thường, tin học hóa không làm thay đổi quy trình đã có hoặc mô hình hoạt động đã có. Khi tin học hóa ở mức cao, dẫn đến thay đổi quy trình hoặc thay đổi mô hình hoạt động, thì gọi là chuyển đổi số.

Chuyển đổi số là gì?

Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số.



Cách mạng công nghiệp lần thứ tư là gì?

- Cách mạng công nghiệp xảy ra khi có đột phá lớn về công nghệ dẫn đến các thay đổi sâu sắc trong sản xuất và xã hội. Cách mạng công nghiệp lần thứ tư được cho là bắt đầu từ thập kỷ này với các đột phá và cộng hưởng của nhiều công nghệ, trong đó có công nghệ số và tạo ra sản xuất thông minh.
- Cách mạng công nghiệp lần thứ nhất là giai đoạn từ cuối thế kỷ XVIII với sự phát minh ra động cơ hơi nước và tạo ra sản xuất cơ khí. Cách mạng công nghiệp lần thứ hai là giai đoạn từ đầu thế kỷ XX với sự xuất hiện của điện lực và tạo ra sản xuất hàng loạt. Cách mạng công nghiệp lần thứ ba là giai đoạn từ những năm 1970 với sự xuất hiện của điện tử, máy tính, Internet và tạo ra sản xuất tự động.