CBS COPENHAGEN BUSINESS SCHOOL

CYBERSECURITY

Introduction

Frejdie Søndergaard-Gudmandsen

Frejdie Søndergaard-Gudmandsen

Cybersecurity

Background

- Head of Product Management at cBrain
- Member of the cyber security policy board at IT-Branchen
- Grand solution impact expert at Innovation Fund Denmark
- External lecturer at University of Copenhagen
- Developer at Nykredit and Miracle

F2

cBRAIN
The Process Company

Course overview

Cyber security lectures

Week	Lecture	Exercise
37	Cyber security	Presentation preperation
38	Attack types and threats	Group presentation
40	AI	Critical thinking
41	Organizational aspects	CFCS gameplay
45	Technical infrastructure	Assignment 3 preparation
46	National security	How to defend vs. attack a country – Blue vs. Red exercise

Learning objectives

- Describe what is cybersecurity
- Discus why is it relevant
- Identify what are we trying to protect
- List and describe some ways that we are trying to protect it
- Know and be able to use the CIA triad for analyzing vulnerabilities

- Preparation for next weeks exercises: Attacks, threats and mitigations

What is cybersecurity?

ERHVERV

Netcompany-værdi i milliardfald efter omfattende hackerangreb

Markedsværdien af Netcompany er høvlet ned med over 1 mia. kroner, siden det blev kendt, at landets største offentlige IT-leverandør er blevet hacket, det skriver Børsen.

Netcompany123! Sådan får du et bedre kodeord end hacket IT-gigant

Netcompany-hack skræmmer eksperter: »Det mest alvorlige, jeg har været vidne til«

PLUS | Ugens Udvalgte | 26. februar kl. 12:31 | 15

What is a cyber attack?

"an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system."

- Internet Engineering Task Force (2000), Internet Security Glossary, RFC 2828, https://datatracker.ietf.org/doc/html/rfc2828

CBS

What is a cyber attack?

An attack: *“Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.”*

A cyber attack: *“An attack, via cyberspace, targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”*

- Committee on National Security Systems of the United States of America (2010), CNSS Instruction No. 4009, https://www.odni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

CBS

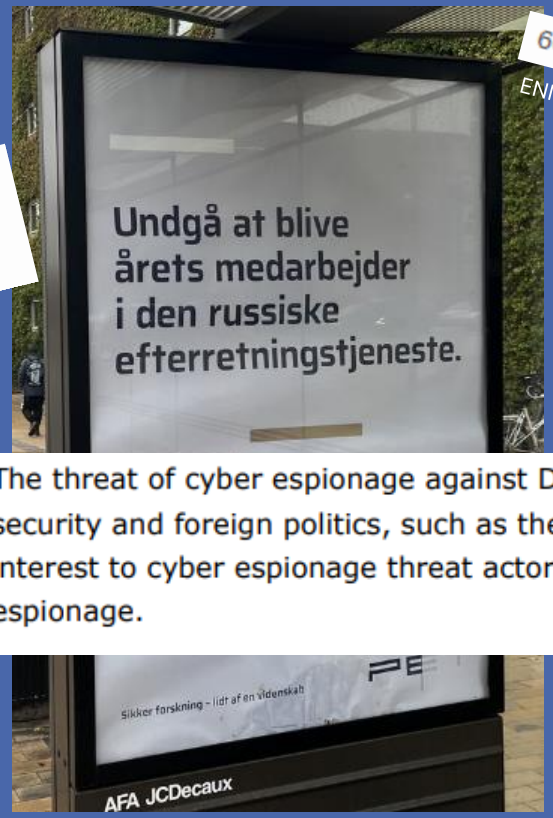
What is cybersecurity?

“the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”

- Oxford dictionary

Why cybersecurity?

The threat of cyber crime against Denmark remains **VERY HIGH**. Well-organized ransomware groups target all levels of society.



66 disclosures of zero-day vulnerabilities observed in 2021

ENISA, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

The threat of cyber espionage against Denmark is **VERY HIGH**. While matters of security and foreign politics, such as the Arctic, NATO and the EU, are of particular interest to cyber espionage threat actors, critical infrastructure is also a target of espionage.

Ransomware attacks, a persistent threat in recent years, are expected to continue their upward trajectory in 2024. Cybercriminals are likely to target not only corporations, but also critical infrastructure and municipal services. The potential for disruption and financial loss remains significant, necessitating organizations to prioritize robust backup solutions, employee training and vulnerability assessments to mitigate the impact of ransomware.

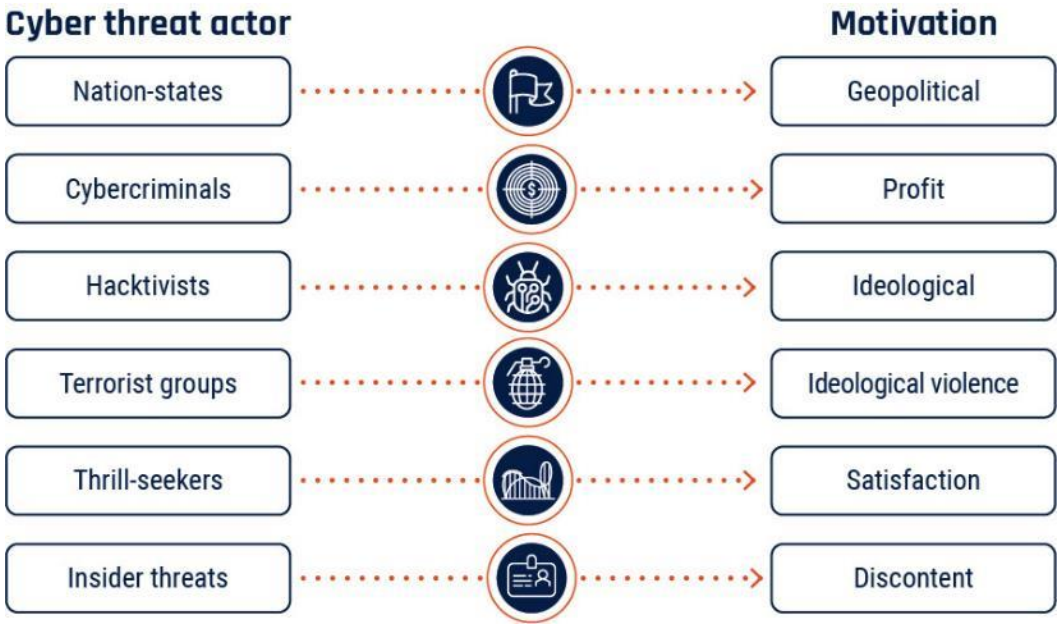
FOBES, https://www.forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/

Beyond AI, 2024 could see record-breaking data breaches. In 2023, the landscape of global data breaches significantly intensified from previous years, including a 72% increase in the number of data compromises over the previous high in 2022.

World Economic Forum, https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/

CBS

Threats actors



Nation-states:

Russia:

- GRU – The Main Intelligence Directorate
- FSB – The Federal Security Service of the Russian Federation
- SVR – Foreign Intelligence Service

China*:*

- PLASSF - Peoples Liberation Army Strategic Support Forces
- CCP MPS – Chinese Communist Party, Ministry of Public Security

Center for Cyber security assesses the Cyber Threat Against Denmark to be very high.

Advanced persistent threat (APT)

Advance persistent threat:

- Actors with unlimited ressources and time
- Long term objectives
- Far reaching capabilities and access to vulnerabilities – such as 0-days

APT 28 – Fancy Bear (RUS)

- Presumed to have close ties with GRU
- The members are connected to Sandworm (NotPetya)

WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS

DETAILS

On October 3, 2018, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against 7 Russian individuals for their alleged roles in hacking and related influence and disinformation operations targeting, among others, international anti-doping agencies, sporting federations, and anti-doping officials. The indictment charges Dmitriy Sergeyevich Badin, Artem Andreyevich Malyshev, Alexey Valerevich Minin, Aleksei Sergeyevich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov, and Ivan Sergeyevich Yermakov, with computer hacking activity spanning from 2014 through May of 2018, including the computer intrusions of the United States Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and other victim entities during the 2016 Summer Olympics and Paralympics and afterwards. The indictment charges these defendants with conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering. The United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

New ministry in Denmark

National security and emergency response

- Newly appointed – 29th of August 2024
- Take parts from many other ministries and agencies
- More than cyber security
- The government takes the threat seriously

For customers in CloudNordic

Unfortunately, during the night of Friday 18-8-2023 at 04 a.m., CloudNordic was exposed to a ransomware attack, where criminal hackers shut down all systems. Websites, e-mail systems, customer systems, our customers' websites, etc. Everything. A break-in that has paralyzed CloudNordic completely, and which also hits our customers hard.

Since we cannot and do not want to meet the financial demands of the criminal hackers for ransom, CloudNordic's IT team and external experts have been working hard to get an overview of the damage and what was possible to recreate.

Unfortunately, it has proved impossible to recreate more data, and the majority of our customers have thus lost all data with us. This applies to everyone we have not contacted at this time.

The hacking attack has been reported to the police.

Status

We are deeply affected by the situation, and are aware that the attack is also very critical for many of our customers. In addition to data, we also lost all our systems and servers and have had difficulty communicating. We have nov re-established blank systems, e.g. name servers (without data), web servers (without data) and mail servers (without data).

Get help to move on without moving

We are ready to **restore customers** on the same name servers with a DNS administration interface, as well as new web servers (without data) and mail servers (without data), so that customers have the opportunity to get mail and the web working again, without moving the domain. Write to support@azero.dk with the word RESTORE in the subject line. In the email, write your email and your phone number as well as the domain, and then you will get logi to a new website and email solution, where you can upload the website yourself and create email addresses.

DIY

Regarding domains where you need to have DNS management quickly:

This is the fastest method to get DNS working again for your domain.

- We have re-established all name service servers, but do not have your DNS zone. Much of the zone can often be copied from https://securitytrails.com/list/keyword > your-domain.xx > Subdomains (very technical).
- If you contact us at support@azero.dk and you are verified as the owner as described below (via email or phone), you can ask us to be created on our name service again, which the domains still point to. You will then get access to a self-service DNS tool (PowerDNS-Admin),where you can do one of the following:
    - Create the DNS zone as you know it should be.
    - Copy zone elements from Securitytrails (see above).

Regarding domains you want moved:

What to do?

- It’s costly to do nothing – but it’s also costly to mitigate
- Prioritize your risks and choose your mitigative actions

10 Minimum Measures

In addition to the four overarching areas of requirement, NIS2 mandates that essential and important entities implement baseline security measures to address specific forms of likely cyberthreats. These include:

- **Risk assessments** and security policies for information systems
- Policies and **procedures for the use of cryptography** and, when relevant, encryption.
- **Security around the procurement of systems** and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.
- **Security procedures for employees with access to sensitive or important data**, including policies for data access. Affected organizations must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
- **The use of multi-factor authentication**, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.
- Policies and procedures for e**valuating the effectiveness of security measures.**
- A plan for handling **security incidents**
- **Cybersecurity training** and a practice for basic computer hygiene.
- **A plan for managing business operations during and after a security incident.** This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
- **Security around supply chains** and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

EU (2024), *NIS2 directive*, https://nis2directive.eu/nis2-requirements/

What is security?

CBS

What are we trying to protect?

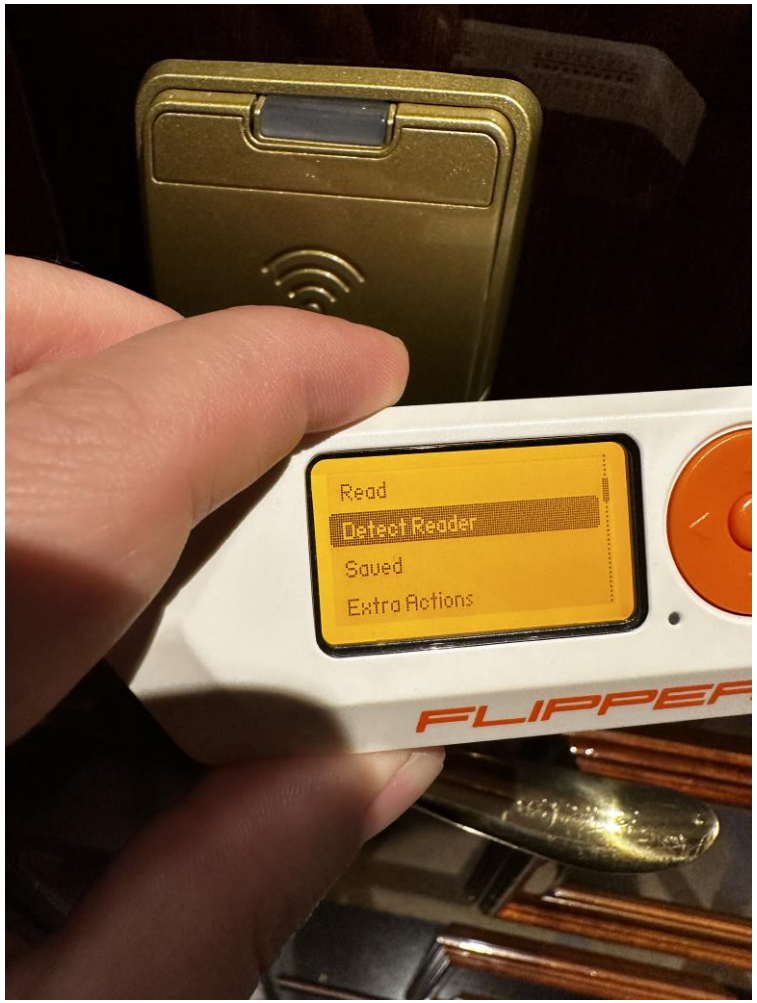
Case: A modern day digital bank

What are we trying to protect?

Case: A hotel

Flipper Zero

Etay Maor, Adjunc professor, Boston College



CBS

Flipper Zero

Etay Maor, Adjunc professor, Boston College

CBS

What are we trying to protect?

Case: The Danish Defence Ministry

What are we trying to protect

It depends!

Threat modelling

- What is the organizations value proposition?
  - Business drivers
  - Business operation
  - Revenue streams
  - Assets (prioritized)
  - Intellectual property (IP) / confidentiality
  - Internal systems / operational resilience

Break

15 min

What is a hacker?

What is a hacker?

- Aka 'ethical hackers'
- Given legal permission, often for a fee to test an organization's computer security system
- Find vulnerabilities that can cause security to be compromised
- Conduct Penetration Testing and Vulnerability Assessments

- Stereotypical type of hackers
- Support criminal acts through their hacking skills
- Illegally attack computer systems for personal gains & ransom
- Using malware to gain acces to sensitive information, steal data & corrupt documents

- Do not have malicious intentions
- Simply trying to gain something for their own findings
- May try to compromise an organization's computer system without permission
- Reports back findings and asking to allow them to fix for a fee

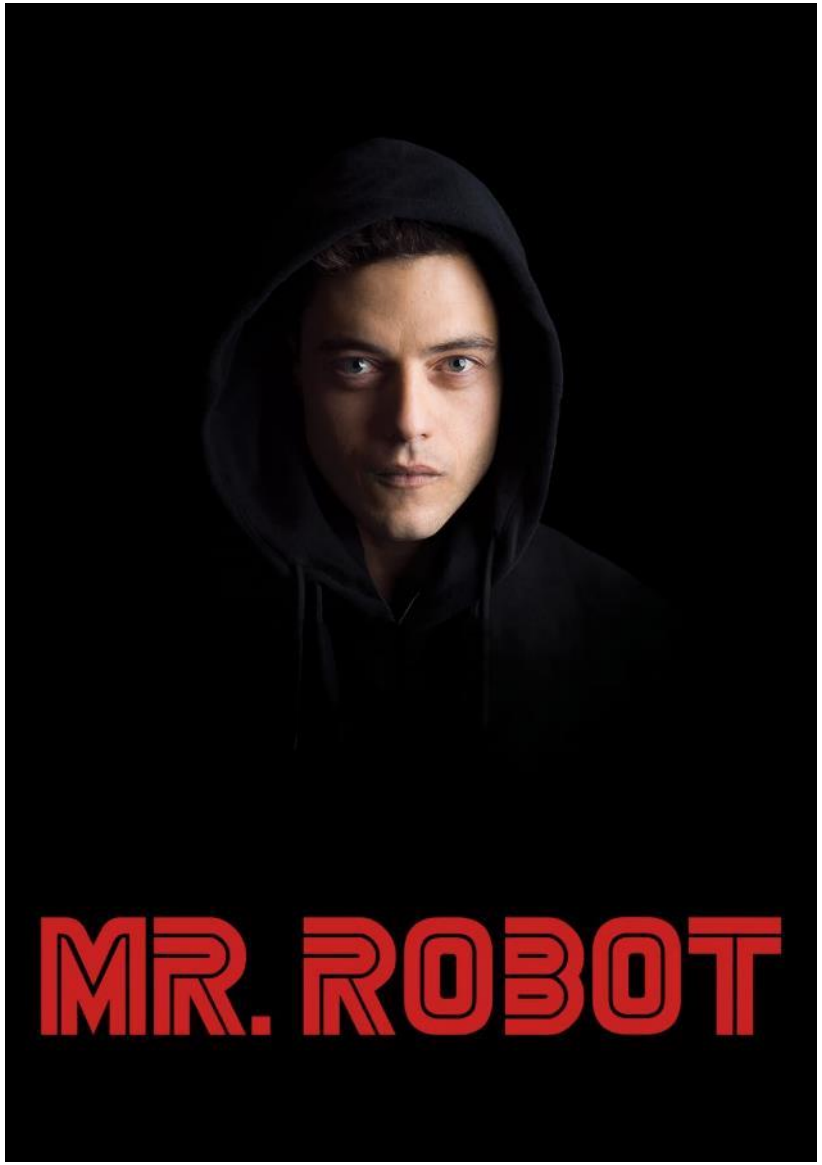
Hackers are all about curiosity, and security is just a feeling

Chris Nickerson | TEDxFultonStreet - https://www.youtube.com/watch?v=HW9hH0vlPEM

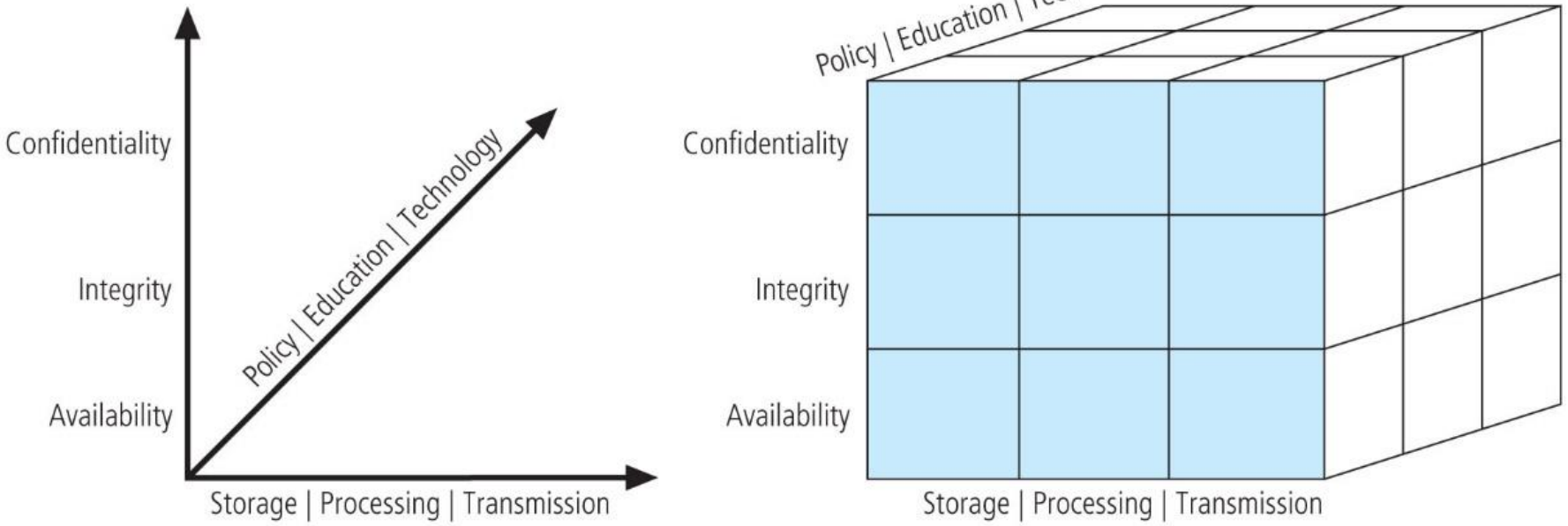
CBS

White hat hacking

- Future job: Pen tester
- For introduction to hands on learning, supplementary exercises can be found a:
  - https://www.hackerone.com/hackers/hacker101
  - https://www.udemy.com/course/learn-ethical-hacking-from-scratch/
- Peter Yaworski (2019), *Real-World Bug Hunting: A Field Guide to Web Hacking*.



The CSNN model and CIA Triad



Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."

Confidentiality

Measures to protect confidentiality

- Information classification (in depth in week 40)
- Secure document (and data) storage
- Application of general security policies
- Education of information custodians and end users
- Cryptography (encryption – in depth in week 45)

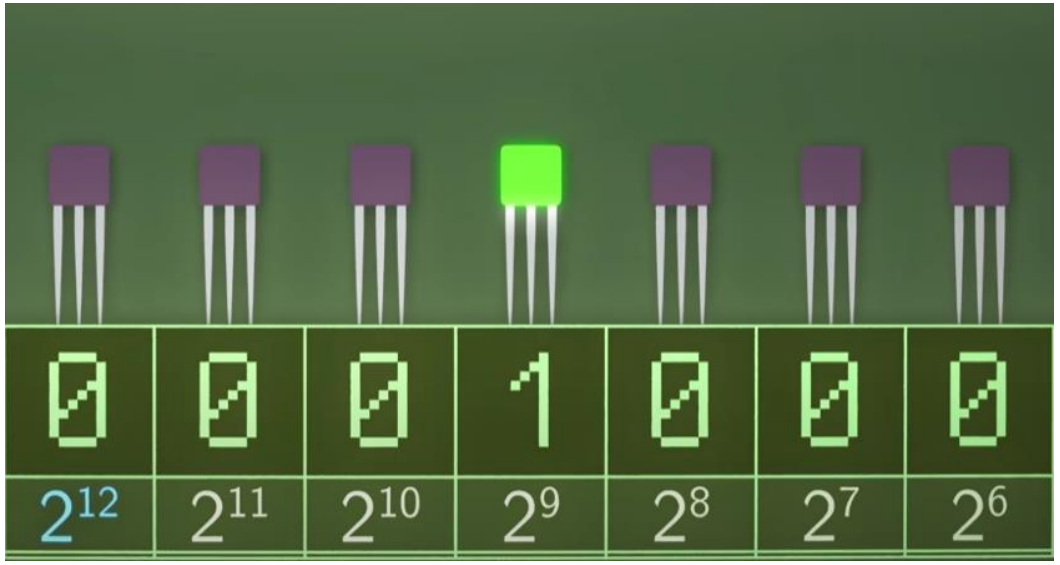
Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."

Integrity

- An attribute of information that describes how data is whole, complete, and uncorrupted
- The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
- Ex: The Universe is Hostile to Computers (23:01 minutes):

https://www.youtube.com/watch?v=AaZ_RSt0KP8&list=PLXHfP9ffsuFe6uBOy-I4k-FWyiZhBEPY6&index=9&t=6s



Integrity

How can we test and ensure the integrity of data?

- State of file (size, time, hash value, etc.)
- Monitoring changes
- Error-control techniques (e.g., redundancy bits and check bits)
  - **Error Detection and Correction Techniques (11:23 minutes):**

https://www.youtube.com/watch?v=GMmnvTV2tI0

Availability

“Ensuring timely and reliable access to and use of information.”

Availability

- Ex. Ransomware, DDOS, power outage etc.
- **Mitigative measurements:**
  - Data backup and restore procedures
  - Network protection tools, load balancers etc. (in depth in week 45)
  - Backup generators

Cybersecurity recap

1. What is valuable to us?
2. What are we afraid of?
3. What can cause the object of our fear?
4. What can we do to prevent or mitigate it?
5. What *should* we do to prevent or mitigate it?
6. How are we going to implement, monitor, evaluate and sustain these preventions?

Questions?

Break

15 min

Exercise

Presentation of a specific attack

ET tech | Unwrapped

NotPetya: the cyberattack that shook the world

Published on 5 Mar, 2022

The country where officials are using pen, paper and typewriters to govern after major cyber-attack

Vanuatu's online public sector was knocked off for nearly a month in a malware attack

Alisha Rahaman Sarkar • Tuesday 29 November 2022 09:14 GMT • Comments

Alma radio telescope in Chile taken down by cyber attack

The Atacama Large Millimeter/submillimeter Array Observatory will be offline for an indeterminate amount of time as workers try to recover from a 29 October cyber attack

Children's addresses leaked in school cyber-attack

4 June 2024

Colonial Pipeline returns to normal operations after shutdown caused by cyberattack

The pipeline supplies nearly half of the East Coast's gasoline and diesel

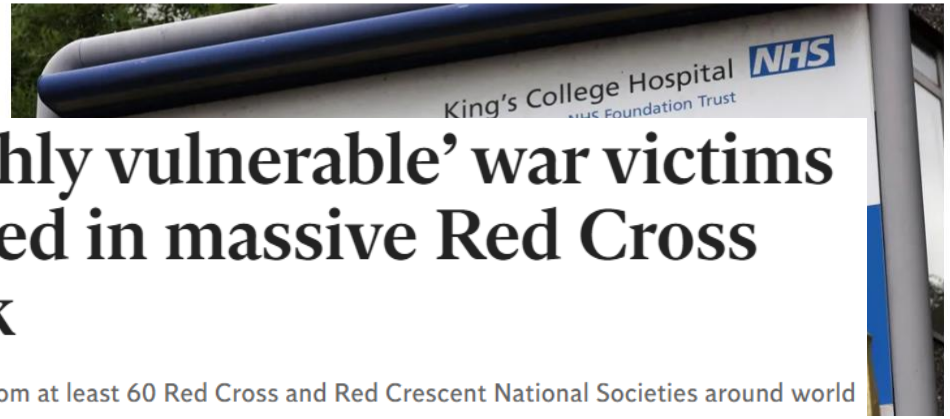
Home News Sport Business Innovation Culture Travel Earth Video Live

NHS confirms patient data stolen in cyber attack

24 June 2024

Share

Ian Casey
BBC News



Data of 'highly vulnerable' war victims compromised in massive Red Cross cyber attack

Compromised data originated from at least 60 Red Cross and Red Crescent National Societies around world

CBS

Exercise

Presentation of a specific attack

- Preparation for next weeks exercise where you are to present your findings
- Form groups of 2-4 students
- Find a real live example of a cyber attack
- Analyze it using the CIA definitions:
  - What was affected?
  - How severe was the effect in relation to the value proposition of the organization? What was the impact?
- Start reading the articles for next week regarding attack types and mitigative actions. Based on this, describe in depth:
  - What type(s) of attack(s) was performed?
  - How. What vulnerability was exploited? What was technically done?
  - What did the organization do to mitigate the attack (both preemptive and after the facts)?
  - What *could* the organization had done to better mitigate the attack? (we'll get back to this later).
- Prepare a 5-8 minutes presentation to be held in class next week.

Exercise

- Register your case on Canvas to ensure the breadth of the cases.
- Note down:
  - Title (attack name, specific company or other significant title)
  - Group members
  - Attack type (rough category)