UNIVERSITAS
GADJAH MADA

Pelatihan Dasar Pengoperasian Sistem
Tenaga Listrik Modern

Cybersecurity Fundamentals

Guntur Dharma Putra, PhD
Slide: Courtesy of Bagus Rakadyanto O. P.

Departemen Teknik Elektro dan Teknologi Informasi
Fakultas Teknik UGM

Who am I

Guntur Dharma Putra, PhD

- Dosen DTETI Fakultas Teknik UGM
- Head of Systems Research Group
- Head of IT Research Facilities
- Asesor BNSP
- Anggota Tim Pokja Blockchain - Metamesta DIKTI
- Anggota IEEE, ACM, PII

Education

- Sarjana Teknik Elektro UGM 🇮🇩
- Master's in Computing Science
  University of Groningen, the Netherlands 🇳🇱
- PhD in Computer Science and Engineering UNSW Sydney,
  Australia 🇦🇺

Research Area

- Distributed systems
- Cyber-physical systems
- Internet of things
- Blockchain
- Security and privacy

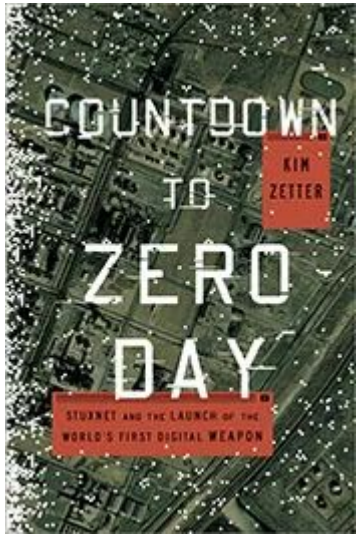
Intro to Cybersecurity

- What is Cybersecurity?
- Why it is important?

What is Cybersecurity?

- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (America's Cyber Defense Agency)
- Cybersecurity -> Encompasses technologies, processes, and policies designed to prevent, detect, and respond to cyber attacks.
- https://www.scirp.org/journal/paperinformation?paperid=121421

Some “Big” Cybersecurity Incident



WIRED **An Unprecedented Look at Stuxnet, the World's First Digital Weapon**

IN JANUARY 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them.

Five months later a seemingly unrelated event occurred. A computer security firm in Belarus was called in to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. Again, the cause of the problem was a mystery. That is, until the researchers found a handful of malicious files on one of the systems and discovered the world's first digital weapon.

Some “Big” Cybersecurity Incident

Malware caused blackouts!

Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world

May 17, 2024
By Emily Cerf

SHARE THIS STORY:

On a cold winter night in 2016, Ukrainians experienced the first-ever known blackout caused by malicious code (malware) designed to autonomously attack the power grid. One-fifth of Kyiv’s citizens were plunged into darkness as attackers used malware to target the capital city’s power grid. Six years later, in the early months of the ongoing Russia-Ukraine war, a second attack attempted to combine kinetic and cyber attacks to take down Ukraine’s power grid.

Power lines in Ukraine. Photo credit: Mny-Jhee, iStock.

Malware attacks against physical infrastructure have long been a looming threat in the realm of cybersecurity, but these two in Ukraine were the first attacks of their kind, and have received little attention from the academic community. Carried out by a Russian intelligence agency against Ukraine, they warn of the evolution of cyber attacks to the built world, and highlight the need to better understand and defend against this type of malware.

Case Study: RTE (France's transmission system operator)

2018 RTE Realibility Report

In 2018, RTE's Operational Security Centre (COrS'R) tackled over 10,000 attacks every month, prevented 3.3 million spam emails and eradicated 200 viruses on RTE's IT system.

2023 RTE Realibility Report

Cybersecurity

The security of RTE's IS is an essential part of the operational reliability of the electricity system, particularly for the industrial IS, but also for the IS for information exchange with customers, market players and partners.

In 2023, risk assessments, external audits and intrusion tests of RTE's information system were carried out to establish the company's level of resilience to cyberattack, and to ensure the continuity of its essential activities. The majority of the key information systems were the subject of detailed studies and now carry internal certification.

The new StanWay system for grid operation and supply-demand balancing was commissioned in 2023: the first months of trial operation were used to rectify a few anomalies and improve system functionality. This finetuning was mostly based on the operators' feedback, but also drew on in-depth analyses of incidents involving StanWay.

RTE is also continuing to renew and develop its telecommunications networks, and to strengthen the cybersecurity of its infrastructure. In 2023, RTE enhanced the use of its system by opening the first of 3 Electricity System Operation Centres (COSE). The setting up of these control centres, which will replace the 7 existing regional dispatch centres, is designed to improve RTE's advance and real-time response capacity, and to address the growing complexity of managing energy flows and supply-demand balancing by streamlining the interactions between areas.

Why it is important?

- Prevent economic losses
- Prevent compromising public safety
- Operational continuity
- Privacy preservation
- Data protection
- Many more...

Core Principles

- CIA Triad
- Applying the Principles

CIA Triad

- Confidentiality
- Integrity
- Availability

CIA Triad: Confidentiality

- Ensuring that sensitive information is accessible only to authorized individuals.
- Effort to make sensitive information kept secret or private

CIA Triad: Confidentiality - Implementation Example

- **Access Controls**: Restricting system access to authorized users.
- **Encryption**: Encoding data to prevent unauthorized reading.
- **Data Masking**: Obscuring specific data elements to protect privacy.
- **MFA**: Multi Factor Authentication system

CIA Triad: Integrity

- Maintaining the accuracy, consistency, and trustworthiness of data over its lifecycle.
- Effort to make sure data is trustworthy and free from tampering.

CIA Triad: Integrity - Implementation Example

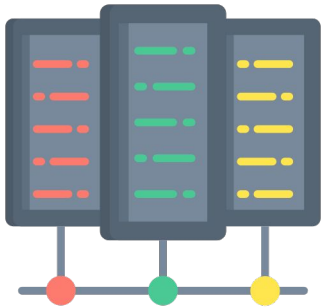
- **Hash Functions**: Generating unique digital fingerprints for data verification.
- **Digital Signatures**: Authenticating the source and integrity of digital messages.
- **Audit Trails**: Keeping detailed records of data access and modifications.

CIA Triad: Availability

- Ensuring that information and resources are accessible to authorized users when needed.
- Even if data is kept **confidential** and its **integrity maintained**, the systems, networks, and applications must be **functioning** as they should and **when they** should.

CIA Triad: Availability - Implementation Example

- **Redundancy**: Deploying multiple systems or components to prevent single points of failure.
- **Load Balancing**: Distributing network traffic to maintain performance during high-demand periods.
- **Regular Backups**: Creating copies of data to restore availability in case of disruptions.



Applying CIA Triad to Critical Infrastructure

- **Confidentiality**: Protecting sensitive operational data and control systems from unauthorized access to prevent espionage or sabotage.
- **Integrity**: Ensuring that data transmitted within and between systems remains unaltered, preserving the reliability of monitoring and control operations.
- **Availability**: Guaranteeing that critical systems and data are accessible to authorized personnel, especially during emergencies, to maintain operational continuity.

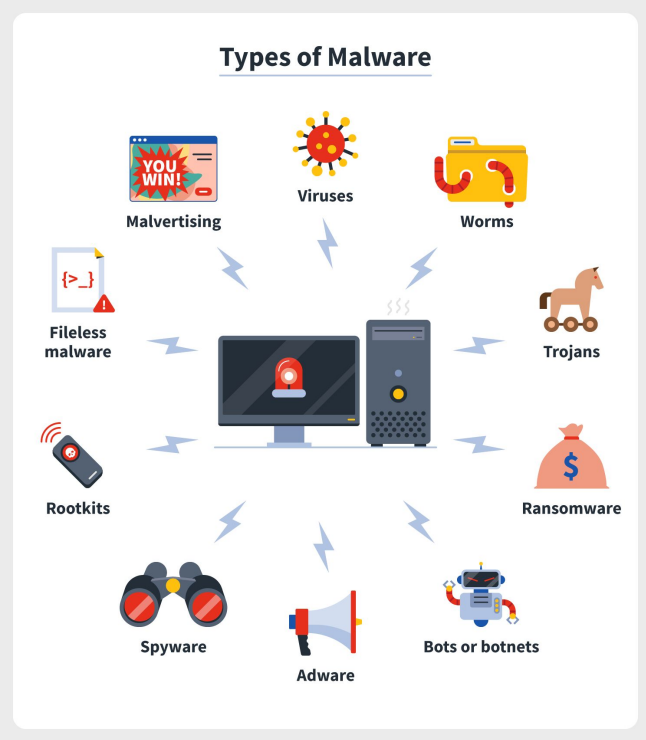
Threat Landscape

Types of Cyber Threat

- Malware
- Phising
- Social Engineering
- Denial of Service (DoS) Attack
- Man-in-the-Middle (MitM) Attack
- Insider Threats

Types of Cyber Threat : Malware

- Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.



Types of Cyber Threat : Malware

- **Viruses**: Attach to files and replicate when executed.
- **Worms**: Self-replicate to spread across networks without user intervention.
- **Trojans**: Disguise as legitimate software to deceive users into installation.
- **Ransomware**: Encrypts data and demands payment for decryption.
- **Botnet**: Malware that gain access to devices through a piece of malicious coding -> remote devices

Types of Cyber Threat : Malware

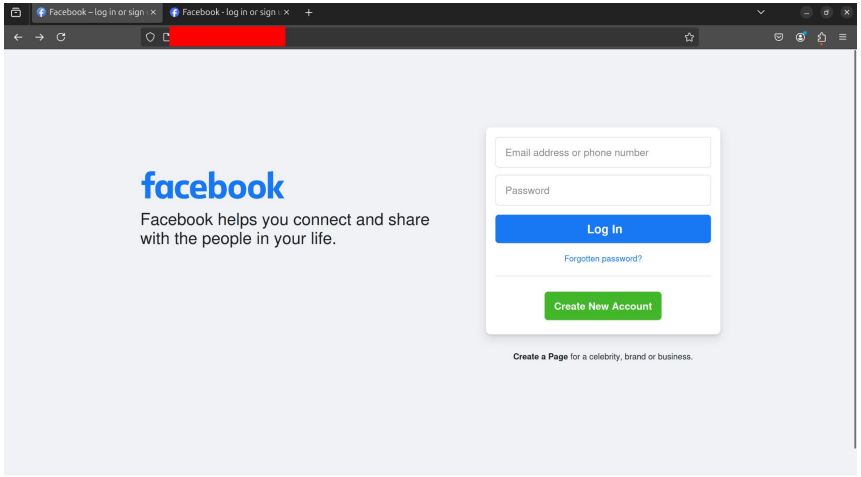
- **Adware**: Display unwanted advertisements
- **Spyware**: Collects information about users without their knowledge.
- **Rootkit**: Gain root remote control victim devices
- **Fileless Malware**: Malware that uses software, applications, and protocols already built-in or native to device operating systems to install and execute malicious activities via memory
- **Malvertising**: malware that comes from ads on legitimate websites

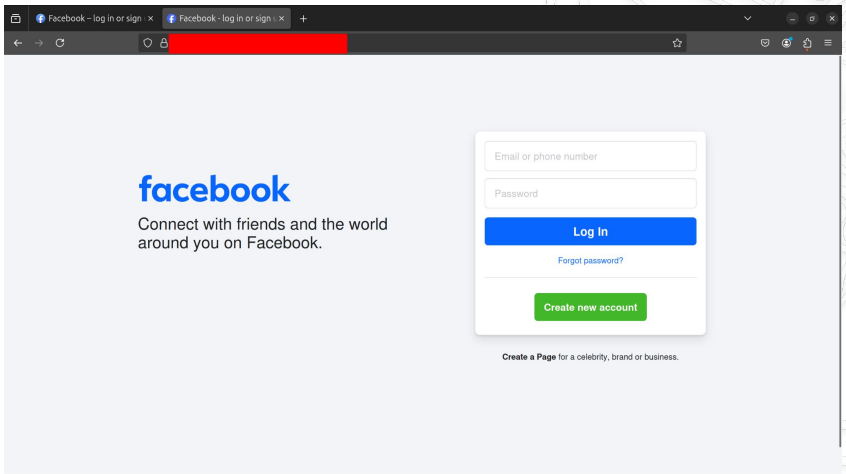
Types of Cyber Threat : Phishing

- Attackers impersonate legitimate entities to deceive individuals into providing sensitive information.

Types of Cyber Threat : Phishing - Web Phishing

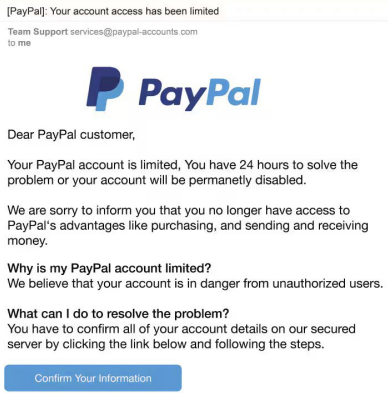
- Can you spot the difference?
- Which one is real?





Types of Cyber Threat : Phishing

- Another Methods:
  - **Email Phishing**: Sending fraudulent emails to trick recipients.
  - **Spear Phishing**: Targeting specific individuals with personalized messages.
  - **Smishing**: Using SMS messages to phish for information.
  - **Vishing**: Conducting phishing attacks via voice calls.


[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

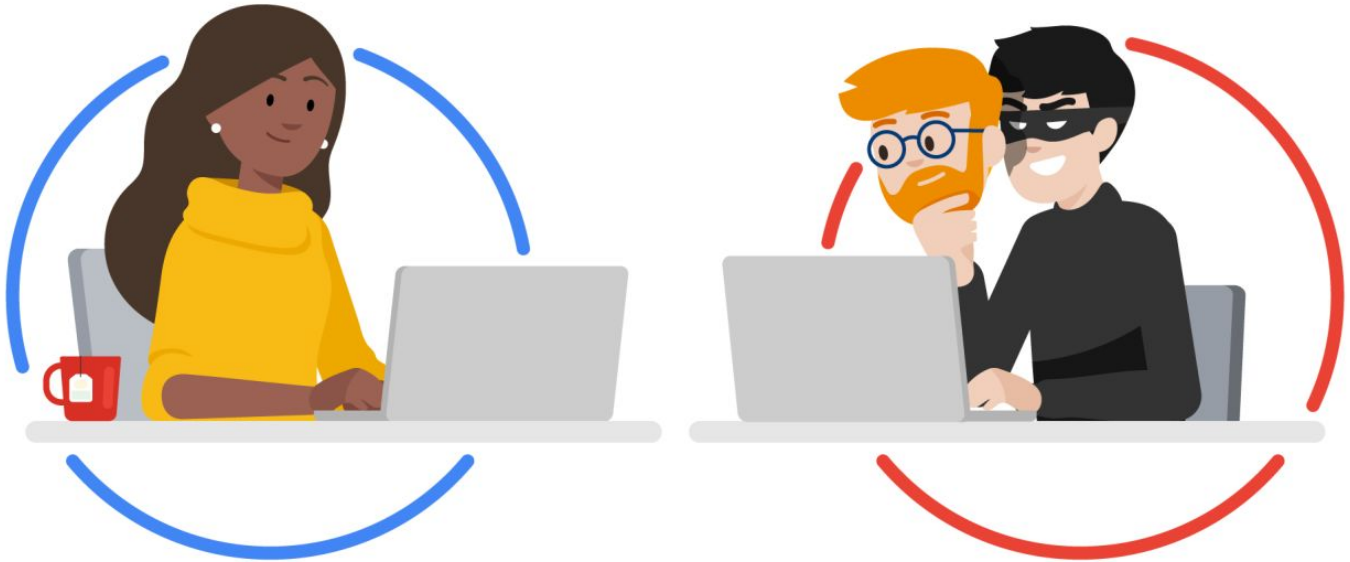
Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

Types of Cyber Threat : Social Engineering

- Psychological manipulation of individuals into performing actions or divulging confidential information.

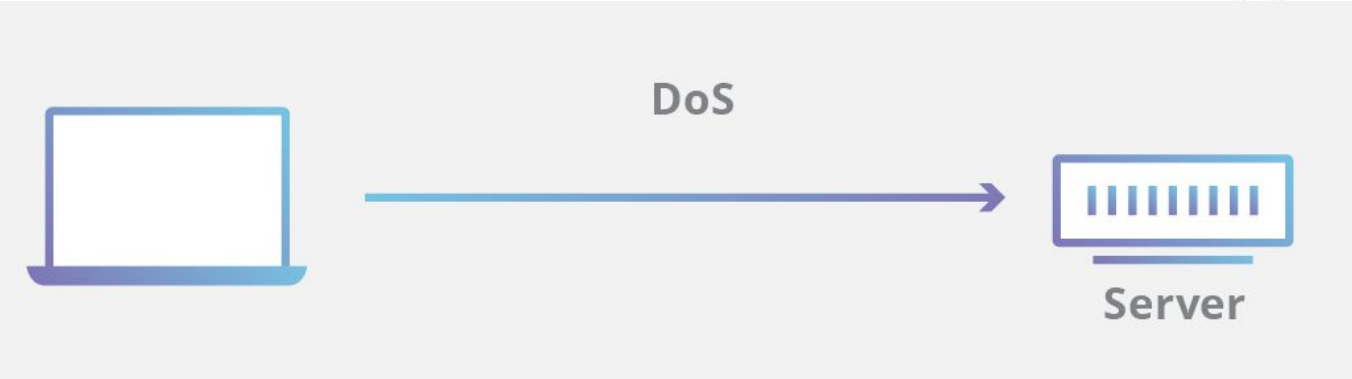


Types of Cyber Threat : Social Engineering

- Examples:

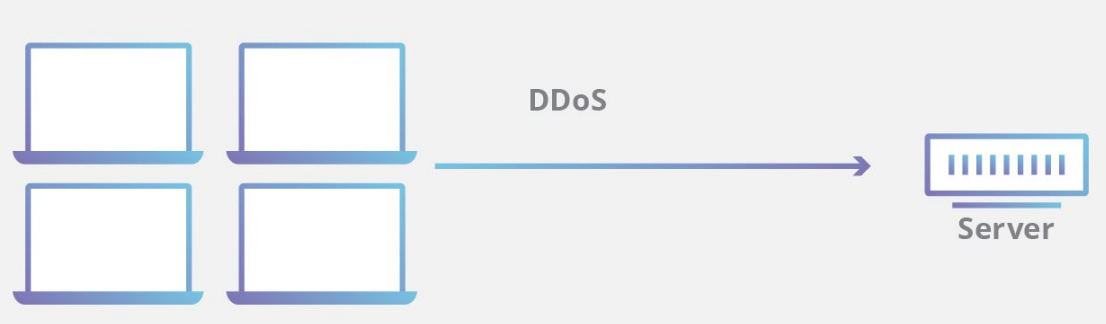
Types of Cyber Threat : DoS Attack

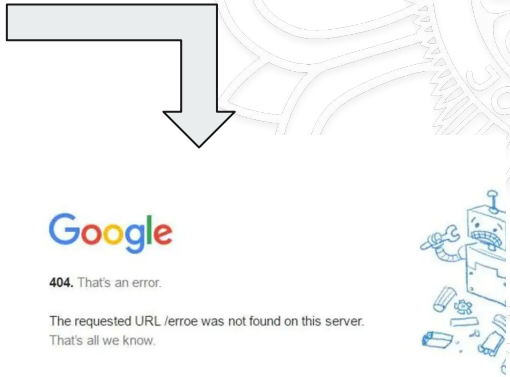
- **Denial of Service (DoS) Attack**: An attack aimed at making a machine or network resource unavailable to its intended users by overwhelming it with traffic.



Types of Cyber Threat : DoS Attack

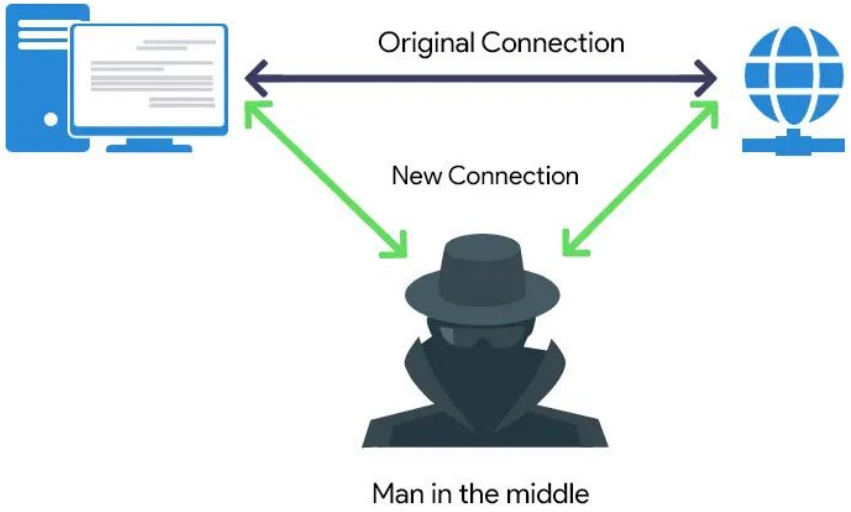
- **Denial of Service (DoS) Attack** -> more practical -> **Distributed Denial of Service (DDoS) Attack**
- DDoS usually uses **botnets**





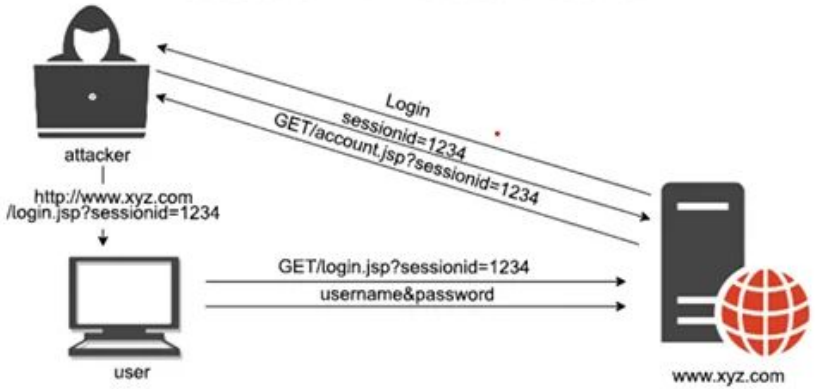
Types of Cyber Threat : Man-in-the-Middle Attack

- An attack where the attacker secretly intercepts and possibly alters data exchanged between two parties.



Types of Cyber Threat : Man-in-the-Middle Attack

- Methods:
  - Session Hijacking: Taking over a user's session to gain unauthorized access.
  - SSL Stripping: Downgrading HTTPS connections to HTTP to intercept data.
  - Wi-Fi Eavesdropping: Intercepting data over unsecured or compromised Wi-Fi networks.

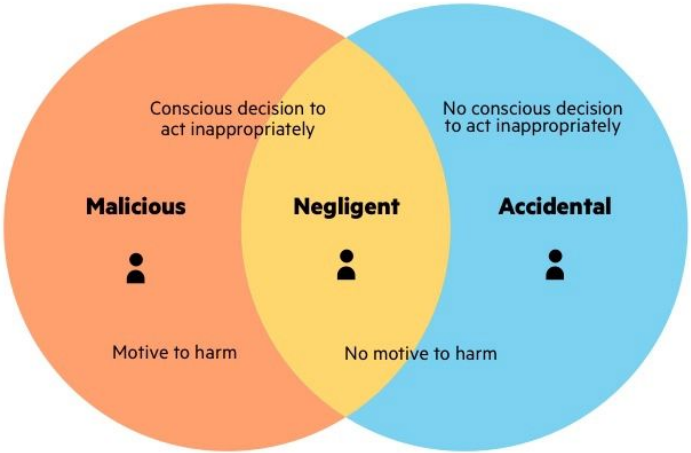


Types of Cyber Threat : Insider Threats

- Threats originating from within the organization, such as employees or contractors, who have access to sensitive information.

Types of Cyber Threat : Insider Threats

- Types:
  - **Malicious Insiders**: Individuals who intentionally misuse their access.
  - **Negligent Insiders**: Individuals who inadvertently cause harm through carelessness.
  - **Accidental Insiders**: Individuals who have done standard operating procedures but still get hacked
  - **Compromised Insiders**: Individuals whose credentials have been stolen and are used by external attackers.



Types of Cyber Threat : Insider Threats

- Indodax Insider Threats Example:

CNBC INDONESIA HOME MARKET MY MONEY NEWS TECH LIFESTYLE SHARIA ENTREPRENEUR

CNBC Indonesia > Tech > Berita Tech

Indodax Diduga Kena Hack, Kerugian Tembus Rp 221 Miliar

Intan Rakhmayanti, CNBC Indonesia

11 September 2024 14:25

Indodax, salah satu platform *exchange cryptocurrency* terbesar di Indonesia telah menghadapi serangan siber pada 11 September 2024. Peretasan ini membuat dana Indodax bernilai lebih dari Rp300 miliar hilang dan akses ke *exchange* tersebut terpaksa dihentikan sementara.

Baca juga: Indodax Konfirmasi Diretas, Siap Tanggung Kerugian Penuh!

Setelah kondisi stabil dan sistem aman, CEO Indodax, Oscar Darmawan, secara terbuka menjelaskan kronologi peristiwa ini dalam *talkshow* Indodax pada Senin (23/9/2024).

Oscar memaparkan bahwa insiden bermula ketika seorang *engineer* Indodax menerima tawaran pekerjaan *freelance* dengan bayaran fantastis.

Engineer tersebut diimingi bayaran ribuan dolar untuk mengatur sebuah server dalam waktu hanya satu jam. Tanpa disadari, tawaran tersebut merupakan tipu muslihat yang digunakan oleh peretas untuk menyusupi sistem Indodax.

"Orang ini bekerja menggunakan laptop kantor dan menyalahi SOP Indodax, ternyata pekerjaan *freelance* ini hanya kedok untuk menyusupi laptop yang dipakai," kata Oscar.

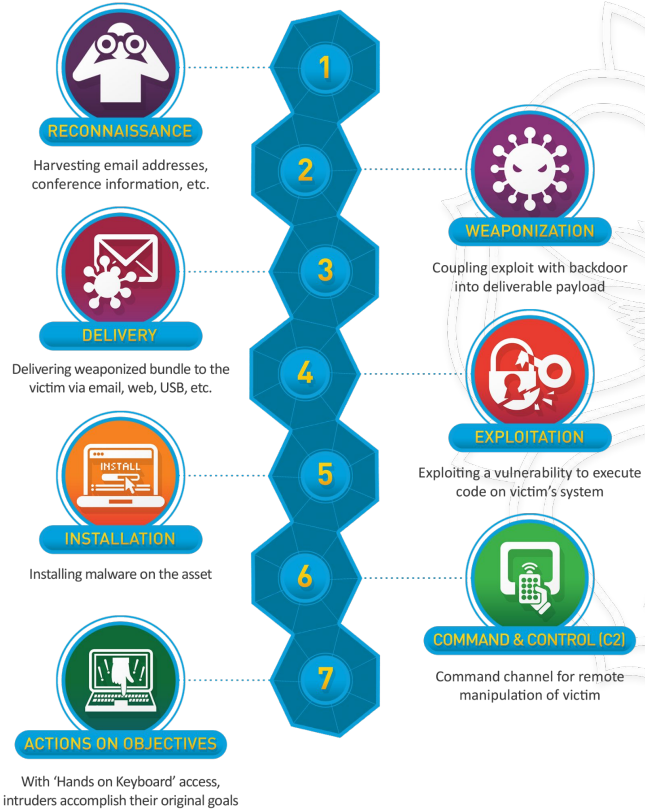
Dalam melakukan pekerjaan tersebut, *engineer* Indodax harus mengunduh sebuah file yang ternyata telah disusupi oleh malware yang dirancang untuk menyerang server perusahaan.

Attack Framework

- Lockheed Martin Cyber Kill Chain
- The MITRE ATT&CK Framework

Lockheed Martin's Cyber Kill Chain Framework

- Developed by Lockheed Martin, the Cyber Kill Chain is a model that outlines the stages of a cyberattack, providing a structured approach to predict and counteract potential threats.

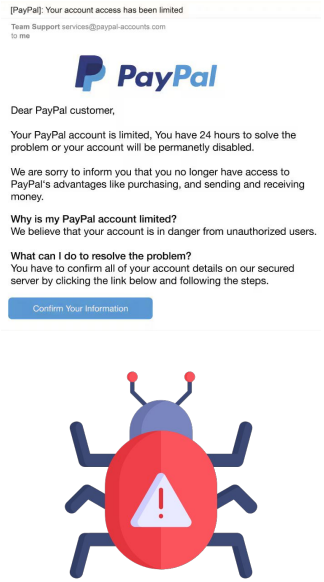


Cyber Kill Chain: Reconnaissance

- Attackers gather information about the target organization to identify potential vulnerabilities.
- Port scanning, email addresses, server information, etc

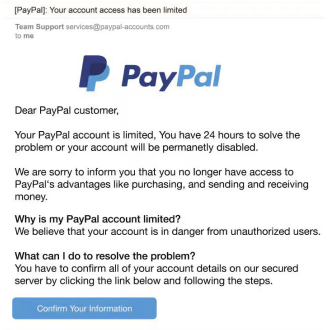
Cyber Kill Chain: Weaponization

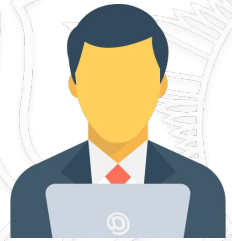
- Creating malicious payloads, such as malware or phishing emails, tailored to exploit identified vulnerabilities.

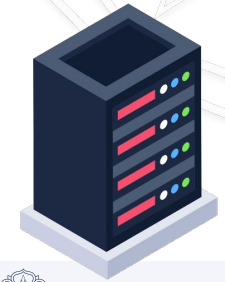


Cyber Kill Chain: Delivery

- Transmitting the malicious payload to the target via methods like email, websites, or USB drives.

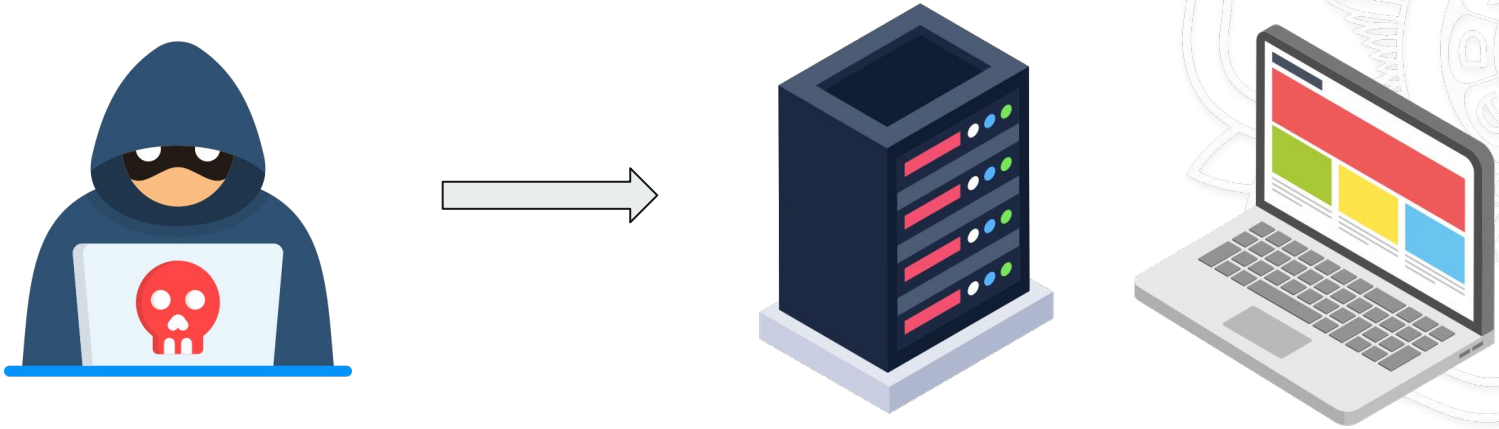






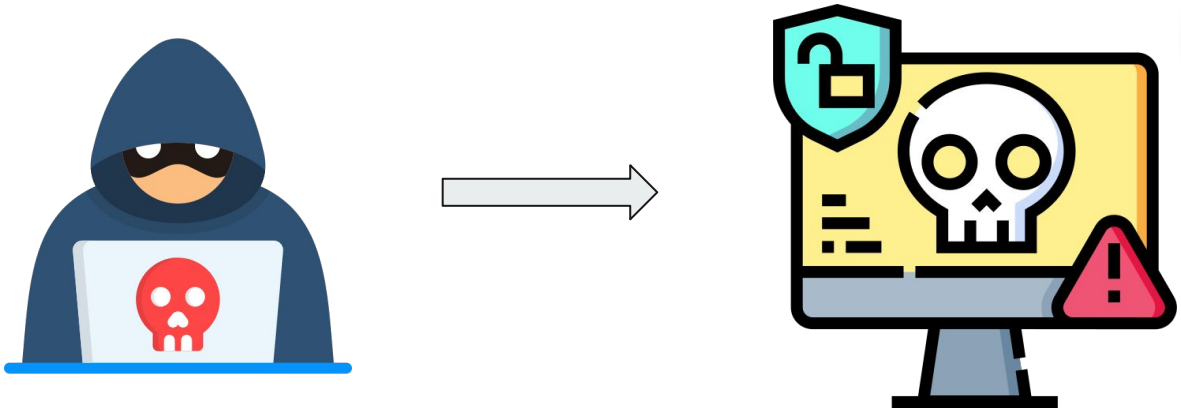
Cyber Kill Chain: Exploitation

- Executing the malicious code to exploit vulnerabilities and gain unauthorized access.



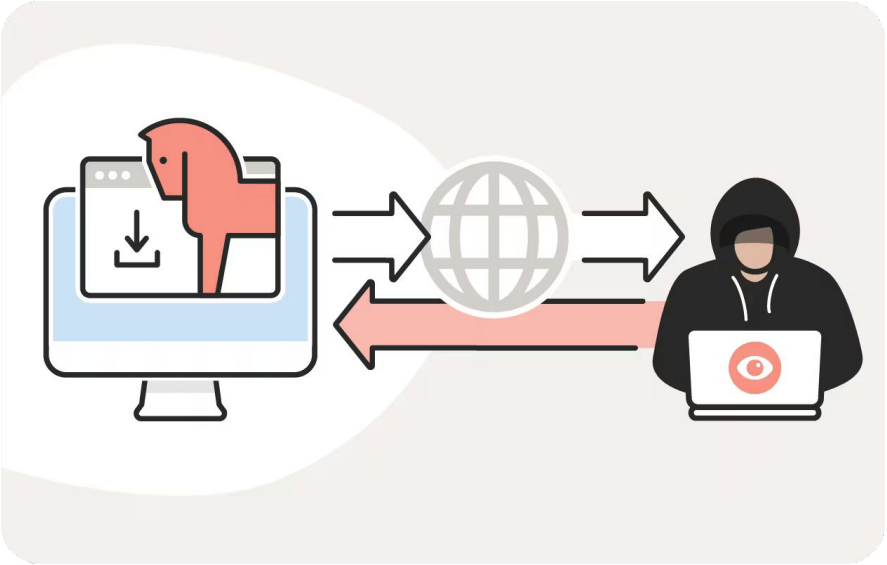
Cyber Kill Chain: Installation

- Installing malware to establish a persistent presence within the target system.



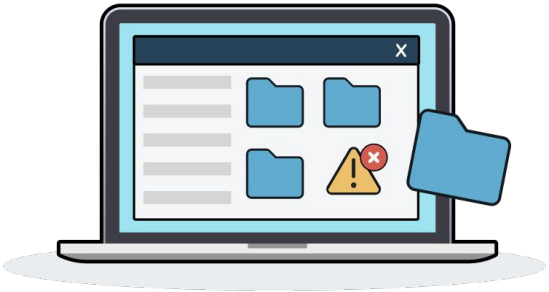
Cyber Kill Chain: Command and Control (C2C)

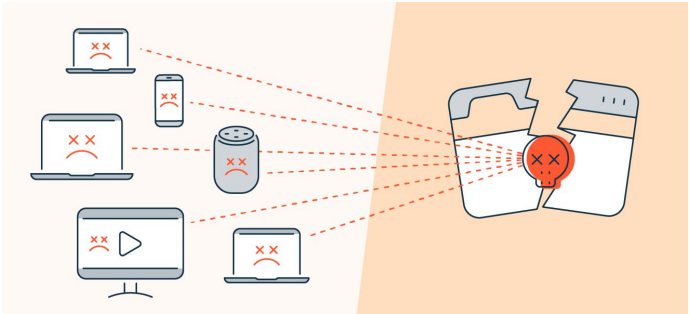
- Establishing communication between the compromised system and the attacker's server for remote control.

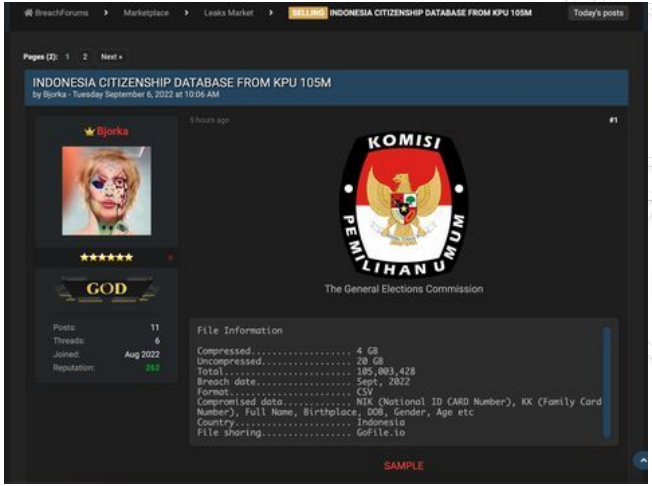


Cyber Kill Chain: Actions on Objectives

- Carrying out the attacker's goals, such as data exfiltration, system damage, or espionage.

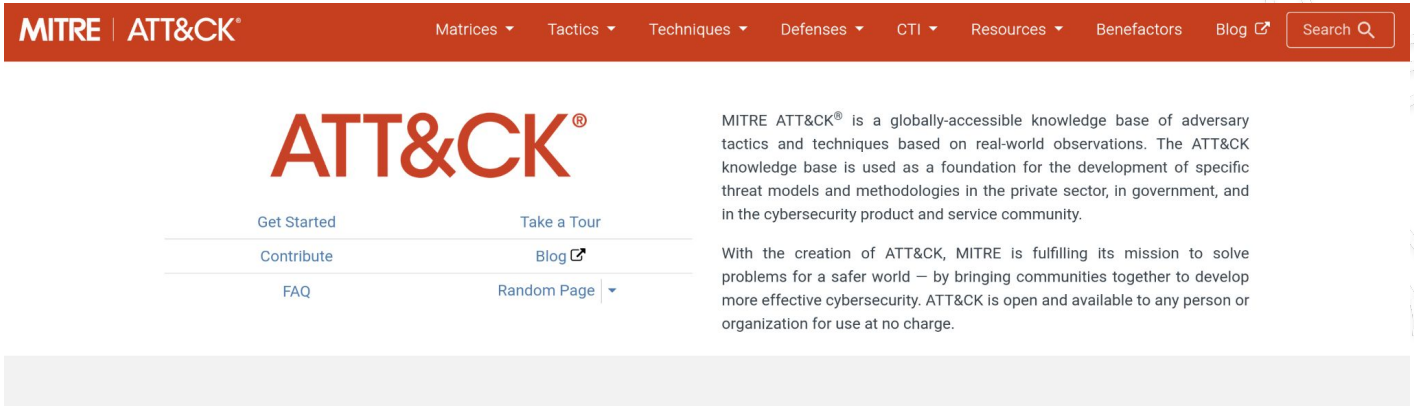






The MITRE ATT&CK Framework

- The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that catalogs adversary tactics and techniques based on real-world observations.



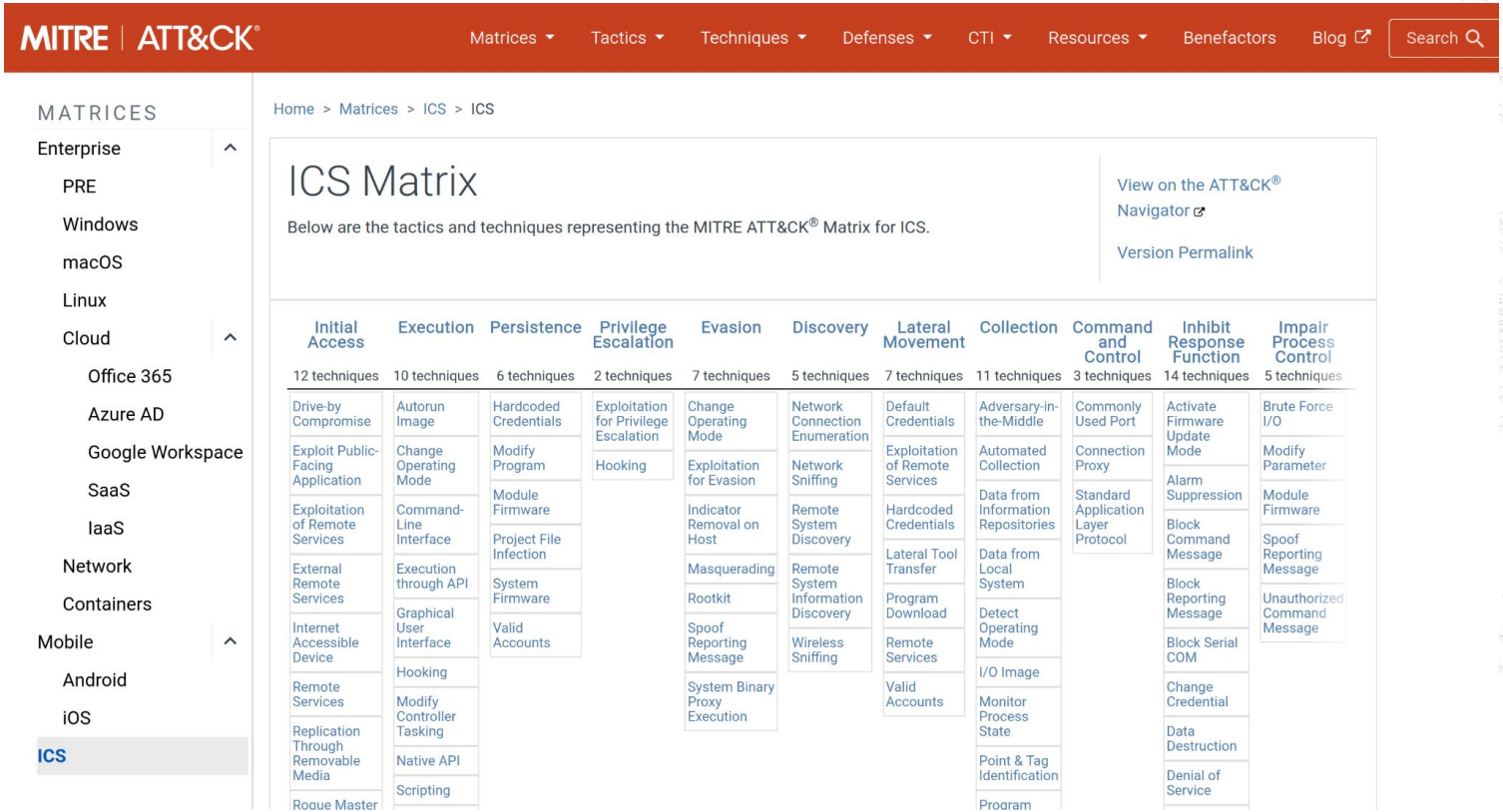
The MITRE ATT&CK Framework

- The framework is organized into matrices, each representing a different domain:
  - **Enterprise**: Covers traditional IT environments, including Windows, macOS, Linux, and cloud platforms.
  - **Mobile**: Focuses on mobile devices and platforms.
  - **ICS**: Pertains to Industrial Control Systems.

The MITRE ATT&CK Framework

- Each matrix consist of
  - **Tactics**: The adversary's technical objectives during an attack (e.g., Initial Access, Execution).
  - **Techniques**: Specific methods used to achieve these objectives.
  - **Sub-techniques**: More detailed breakdowns of techniques.

The MITRE ATT&CK Framework



What these two attack frameworks are for?

- Develop threat models and methodologies.
- Enhance detection and response strategies.
- Conduct adversary emulation and red teaming exercises.
- Assess and improve security posture by identifying coverage gaps.

Comparing the Frameworks

- **Focus**: The Cyber Kill Chain provides a high-level overview of the stages of an attack, while the MITRE ATT&CK framework offers detailed information on specific tactics and techniques used by adversaries.
- **Application**: The Cyber Kill Chain is useful for understanding the progression of an attack, whereas the MITRE ATT&CK framework assists in developing specific detection and mitigation strategies.

Key Security Frameworks and Standards

- NIST Cybersecurity Framework
- ISO/IEC 27001
- CIS Controls

NIST Cybersecurity Framework

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a voluntary guidance designed to help organizations manage and reduce cybersecurity risks.
- It provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders.
- The latest version, CSF 2.0, was released in February 2024.

NIST
National Institute of Standards and Technology

NIST Cybersecurity Framework: Core Component

- The CSF is organized around six key functions:
  - **Identify**: Develop an understanding of organizational context, resources, and risks.
  - **Protect**: Implement safeguards to ensure critical services are delivered.
  - **Detect**: Develop activities to identify cybersecurity events.
  - **Respond**: Implement plans to respond to detected cybersecurity incidents.
  - **Recover**: Maintain plans for resilience and restoration of services.
  - **Govern**: Establish and communicate organizational cybersecurity policies and procedures.

NIST Cybersecurity Framework: Implementation

- Organizations can **customize** the CSF to their specific needs, aligning it with **existing processes** and **risk management** strategies.
- The framework also provides informative references to other standards and guidelines, facilitating integration with various cybersecurity practices.

ISO/IEC:27001

- ISO/IEC 27001 is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).
- It aims to help organizations manage sensitive information systematically and securely.

ISO/IEC:27001 - Key Components

- **Context of the Organization**: Understanding internal and external issues relevant to the ISMS.
- **Leadership**: Top management commitment and leadership in establishing the ISMS.
- **Planning**: Addressing risks and opportunities, setting information security objectives.
- **Support**: Providing resources, competence, awareness, communication, and documented information.

ISO/IEC:27001 - Key Components

- **Operation**: Implementing and controlling the processes needed to meet ISMS requirements.
- **Performance Evaluation**: Monitoring, measurement, analysis, evaluation, internal audit, and management review.
- **Improvement**: Addressing nonconformities and implementing continual improvement.

ISO/IEC:27001 - Controls

- ISO/IEC 27001 lists 93 controls organized into four themes:
  - **Organizational Controls**: Policies, procedures, and organizational structures.
  - **People Controls**: Screening, terms and conditions of employment, awareness, education, and training.
  - **Physical Controls**: Secure areas, equipment security, and environmental controls.
  - **Technological Controls**: Network security, access control, and system acquisition.

CIS Control

- The Center for Internet Security (CIS) Controls are a set of best practices for securing IT systems and data against cyberattacks.
- They are developed and maintained by a global community of cybersecurity experts and are updated periodically to address emerging threats.

CIS Control - Version 8

- The latest version, CIS Controls v8, includes 18 controls that are outcome-based and aligned with current technologies and evolving threats.
- These controls are organized into three Implementation Groups (IGs) to help organizations prioritize implementation:
  - IG1: Basic cyber hygiene; essential for all organizations.
  - IG2: Builds upon IG1; for organizations with moderate resources and risk exposure.
  - IG3: Builds upon IG2; for organizations with significant resources and risk exposure.

CIS Control - Key Controls

- **Inventory and Control of Enterprise Assets**: Actively manage all hardware assets.
- **Inventory and Control of Software Assets**: Actively manage all software assets.
- **Data Protection**: Protect data throughout its lifecycle.
- **Secure Configuration of Enterprise Assets and Software**: Establish and maintain secure configurations.
- **Account Management**: Use processes and tools to assign and manage access rights.

Key Takeaways

- Cybersecurity
- CIA Triad
- Cyber Threat Landscape
- Attack Framework
- Security Framework and Standards

UNIVERSITAS
GADJAH MADA

Thanks!

“It takes 20 years to build a reputation and five minutes to ruin it.”
– Warren Buffet –