**Defense in Depth: A Layered Security Approach**

**What is Defense in Depth?**

* A **multi-layered security strategy** that ensures if **one barrier fails**, another is in place to stop an attack.
* Inspired by **medieval castles**, which used multiple defenses like **moats, stone walls, and watchtowers** to slow down and stop attackers.

**Five Layers of Defense in Depth**

1. **Perimeter Layer (Authentication)**
   * The **outermost layer** that filters **external access** to systems.
   * **Security Controls**:
     + Usernames & Passwords
     + Basic Authentication
2. **Network Layer (Authorization & Firewalls)**
   * Focuses on controlling **who can communicate** over the network.
   * **Security Controls**:
     + Firewalls
     + Network Segmentation
     + Intrusion Detection Systems (IDS)
3. **Endpoint Layer (Device Protection)**
   * Protects **devices** (laptops, desktops, servers) that connect to the network.
   * **Security Controls**:
     + Anti-virus software
     + Device encryption
     + Endpoint Detection & Response (EDR)
4. **Application Layer (User Interaction Security)**
   * Secures **applications and software** that process data.
   * **Security Controls**:
     + Multi-Factor Authentication (MFA)
     + Secure Coding Practices
     + Web Application Firewalls (WAF)
5. **Data Layer (Protecting Sensitive Information)**
   * Focuses on securing **critical data** like personally identifiable information (PII).
   * **Security Controls**:
     + Data Encryption
     + Access Control Policies
     + Asset Classification

**Key Takeaways**

* **Each layer strengthens security** by addressing different vulnerabilities.
* **Data moves through all five layers**, making layered security critical.
* **Organizations use this model** to **reduce risks** and **protect important assets**.

**Common Vulnerabilities and Exposures (CVE) and Security Databases**

**Vulnerabilities vs. Exposures**

* **Vulnerability**: A **weakness** in a system that can be exploited by a threat.
* **Exposure**: A **mistake** that creates an opportunity for a threat.

Example:

* A **document** left near an open window is exposed to being **blown away**.

**The CVE List (Common Vulnerabilities and Exposures)**

* A **public dictionary** of known security flaws.
* Created by **MITRE Corporation** in 1999.
* Used by organizations to **identify and mitigate security risks**.
* **Anyone can report** a vulnerability, but it must pass a strict **review process**.

**CVE Review Process & Criteria**

Before assigning a **CVE ID**, vulnerabilities must meet four conditions:

1. **Independence** – Can be fixed without addressing other flaws.
2. **Recognized Risk** – Reporter must acknowledge its security impact.
3. **Supporting Evidence** – Requires documentation or proof.
4. **Single Codebase** – Affects only one system/version.

**NIST National Vulnerability Database (NVD) & CVSS Scoring**

* NVD **analyzes CVEs** further and assigns a **severity score** using **CVSS (Common Vulnerability Scoring System)**.
* **Scoring Scale (0-10):**
  + **0-3.9** → Low Risk (Not urgent)
  + **4.0-6.9** → Medium Risk
  + **7.0-8.9** → High Risk
  + **9.0-10** → Critical Risk (Immediate attention required)

**Why Security Teams Use CVE Lists & CVSS Scores**

* Helps **prioritize security patches** and updates.
* Provides **global insights** into cybersecurity threats.
* Supports organizations in **making informed security decisions**.