CHAPTER 1: SECURITY PRINCIPLES

Ano ang Security?

- Ang security ay proseso ng pag-maintain ng tamang level ng perceived risk o panganib.
- Hindi ito isang resulta kundi isang tuloy-tuloy na proseso.

Mga Hakbang sa Security Process:

1. **Assessment:**
    - Paghahanda para sa iba pang hakbang.
    - Kasama dito ang policies, procedures, laws, at technical evaluation.
    - Kapag may nakaligtaan dito, naapektuhan ang buong operasyon.
2. **Protection:**
    - Paglalagay ng countermeasures para mabawasan ang tsansa ng kompromiso.
    - Ang layunin ay iwasan ang pag-fail, pero lahat ng prevention may limitasyon.
3. **Detection:**
    - Pagkilala sa intrusions o paglabag sa policy.
    - Halimbawa, pag-detect ng unauthorized activities sa network.
4. **Response:**
    - Pag-validate ng detection at pag-ayos ng damage.
    - Puwedeng "patch and proceed" (ayusin lang ang damage) o "pursue and prosecute" (habulin ang may sala).

Key Terms:

- **Risk:** Sukatan ng panganib sa isang bagay na mahalaga.
- **Threat:** Mga tao o grupo na may kakayahan at layuning magsamantala sa kahinaan ng isang asset.
    - **Structured Threats:** May malinaw na layunin, sponsor, at plano (hal., criminals o spies).
    - **Unstructured Threats:** Walang malinaw na layunin, curiosity lang o random malware.
- **Exploit:** Pamamaraan para makasira o makompromiso ang isang asset.
- **Vulnerability:** Kahinaan sa isang bagay, maaaring sanhi ng maling design o implementation.
- **Asset Value:** Halaga o resources na kailangan para palitan o ayusin ang isang bagay na mahalaga.

SECURITY PRINCIPLES: PHASES OF COMPROMISE

Mga Hakbang ng Intrusions:

1. **Reconnaissance (Pagmamasid):**
    - Pagsusuri ng koneksyon at paghahanap ng kahinaan ng target.
    - Mahalaga ito para maintindihan ng attacker ang target at magplano ng atake.
    - **Teknik:**
        - **Passive:** Pagkuha ng impormasyon nang hindi nakikialam (hal., footprinting, banner grabbing).
        - **Active:** Direct interaction tulad ng port scanning at vulnerability scanning.
2. **Exploitation (Pagsamantala):**

    - Pag-abuso o pagsira ng serbisyo.
    - Halimbawa, maling paggamit ng system para sa masamang layunin.
3. **Reinforcement:**
    - Pagpapatibay ng access, tulad ng pagtaas ng privileges sa system.
4. **Consolidation:**
    - Pag-kontrol sa system gamit ang backdoor.
5. **Pillage:**
    - Ang final na layunin, tulad ng pagnanakaw ng data o paggawa ng mas malalaking atake.

LESSON 3: BUSINESS CONTINUITY PLAN

Ano ang Business Continuity Plan (BCP)?

- Ito ay plano na may kasamang resources, procedures, at impormasyon para maipagpatuloy ang operasyon kahit may aberya.

Checklist:

1. **Emergency Contacts:** Listahan ng tao na dapat tawagan kapag may emergency.
2. **Relocation Strategy:** Planong ilipat ang operasyon sa ibang lugar kung kinakailangan.
    - Mga hakbang: tukuyin ang bagong location, backup ng data, at relocation ng empleyado.
3. **Risk Management Plan:** Identipikasyon at pag-manage ng posibleng risks.
4. **Specialized Equipment:** Tukuyin ang critical na gamit sa operations at gumawa ng backup plan.
5. **Vital Documents:** Siguraduhing naka-backup ang mahahalagang files at accessible kahit offline.

LESSON 4: BUSINESS MODEL CANVAS

Ano ang Business Model Canvas?

- Tool para gumawa at magpakita ng business model.
- May 9 na bahagi:
    1. **Customer Segments:** Mga target customers.
    2. **Value Proposition:** Mga benepisyo o solusyon na ino-offer.
    3. **Channels:** Paano inaabot ang customers (hal., online o physical stores).
    4. **Customer Relationships:** Paano mapanatili ang connection sa customers.
    5. **Revenue Streams:** Paano kumikita ang negosyo (hal., sales, subscriptions).
    6. **Key Resources:** Mahahalagang assets (physical, intellectual, human resources).
    7. **Key Activities:** Mga importanteng gawain para magtagumpay ang negosyo.
    8. **Key Partners:** Mga suppliers o partners na tumutulong sa negosyo.
    9. **Cost Structure:** Ang mga pangunahing gastusin sa operasyon.