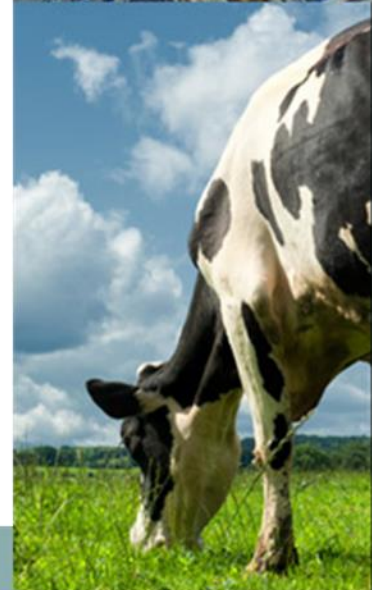הלשכה המרכזית לסטטיסטיקה
Central Bureau of Statistics
دائرة الإحصاء المركزية

Remote Access System and Research Room

Haim Plahchinsky

Agenda

- System Definitions

- Layers security model

- Main system threats

- Concept of work

- Information security requirements
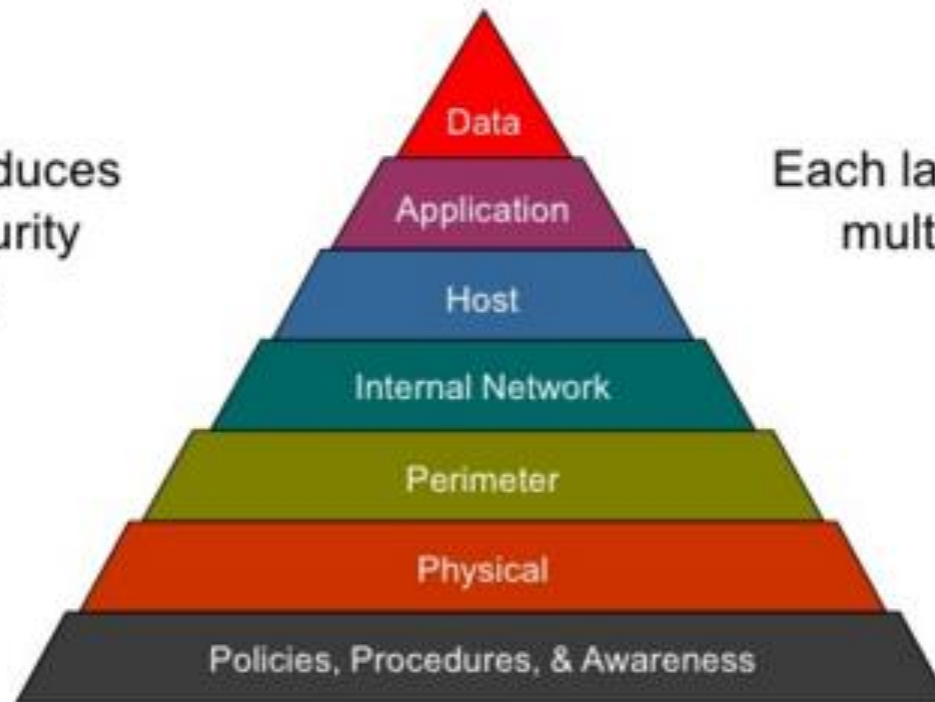
System Definitions

- To establish a simple & friendly system that will make micro-data access for researchers simple without compromising the Confidentiality and privacy of data.

- To enable remote access to MUC data from any computer and any place .

- To enable an access to research room data from dedicated & secured rooms .

Layers security model

Main System Threats

Main System Threats

- **Compromising confidentiality of data**.
  - Hacker.
  - Researcher :by mistake\ without his awareness \ on purpose.
  - Research results exposure by using emails.

- **Denial of service**
  - The researcher by mistake
  - Hackers
  - **Lawsuit**
  - Individual Privacy violations
  - Commercial data exposure

- **Reputation Damage**

Concept of work

- One system that contains MUC & research room information.

- Information will be transferred only after confidentiality board approval.

- User utilization will apply only for authorized researcher that signed NDA & Terms of Use.

- Remote access will apply <u>only</u> for MUC data.

- Access to research room information will be permitted only from dedicated rooms.

- Each research will have designated work space for all researchers.

- There won't be any transfer of research data between projects.

- Export of data only * after verification of data confidentiality .

- CBS professionals can access the system from CBS external Net.

Information security requirements

- Topology
  - separate network
  - FW- to separate the network from internet
  - DMZ zone
    - proxy
    - secure access
  - Second FW to separate the secure access gateway from reaserch servers - VDI component(LAN).
  - IPS module

- LAN zone
  - Divided into segments:
    - OOB management
    - Servers
    - Security
    - MUC data: DB, file server
    - Research room data :DB file server
    - Storage
    - Researchers workstations
    - CBS Professional unit workstations

Information security requirements (III)

- 2 levels authentication.

- Researcher workstation
  - Health / clean check (active X)
  - *windows to go live drivers (e.g SPYRUS)

- SSL VPN – encrypt traffic over the Internet

- Only secure access communicate with the LAN

- VDI – virtual desktop to each researcher.

- Information always stays in the secure zone.

- *Emails limited to sending but not recieving (after check).

Information security requirements (IV)

- Protection module
  - FW
  - DBFW
  - Antivirus
  - Servers hardening
  - segmentation
  - Access approval
  - User managment
  - Patch managment through PROXY.

Information security requirements (V)

- Audit & Detection Modules
  - Recording* activity to prevent non repudiation & unusual behavior
  - LOG and Event Management
  - Honeypot
  - DLP*
- Response module
  - *Available employee
  - IPS
- Data management
  - Unidentified data , each research has individual key.
  - Carefully categorize the data according to damage potential.

Information security requirements (VI)

○ Physical security

- In university
- At CBS
- At Ministries / public bodies