SECURITY

(UNIT-5)

①

combination of availability, confidentiality & integrity focused on the recognition & resistance of attacks.

various reasons for comitting crime against IT:

→ personal exposure & prestige

→ financial, damaging org, Terrorism, warfare

- **Risk Management**

Process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to acceptable level, & maintaining that level.

A risk list used to quantify risks, compiled in Bus Imp Analysis (BIA) workshop, containing:

→ Asset name: component that needs to be protected

→ Vulnerability: a weakness, process or physical exposure that makes asset susceptible to exploits.

→ Exploit: a way to use vulnerabilities to attack an asset

→ Probability: estimate of likelihood of occurence of an exploit

→ Impact: Severity of damage when vulnerability is exploited

→ Risk = P x I

* Controls mitigate these risks

AVE	PIR

→ Risk Response

→ Acceptance of risk: Risk is unlikely & cost of mitigatn is high

→ Avoidance ——.

→ Transfer ——.

→ Mitigation of risk:

→ Design for minimum risk

→ Incorporate * safety devices (Firewalls, Hardened screen routers, P same but I ↓) * warning devices (Intrusion detection system, warn for unusual sitn)

→ Implement training & procedures: mitigate people bound risks

→ Exploits

* key loggers installed (steal password)

* Disposed PCs / disk in wrong h.

* Data on backup tapes outside building in wrong h.

* Corrupt / dissatisfied staff

* N/W sniffers

* End users led to malicious websities stealing info (Phishing)

→ Security controls

Three core goals of security: CIA

→ Confidentiality: prevents unauthorized disclosure of data

→ Integrity: ensures-

* No modifns on data by unauth staff or pr.

* Unauth mod to data not by auth staff or pr.

* Data is consistent

→ Availability: reliable & timely access to data or resources by staff.

* controls based on risk lists & CIA classificn (Risk level determines what level of CIA needed)

→ Attack Vectors

Attacks on infra can be executed using:

⇒ malicious code : App^{ns}, when executed can cause N/w or server overload, steal data & passwords, or erase data

multiple forms:

- → worms: self replicating programs that spread from one comp to another
- → virus: ——— program fragment that attaches itself to a program or file, spreading & leaving infections
- → Trojan horse: appear to be legit files from legit src, hence receiver tricked to start them, & then they deliver viruses or worms.

* Detecting viruses is done using virus signature, a unique string of bits that identifies a part of the virus.

* Heuristic scanning is also used, which looks for certain instruc^{ns} or commands within a program that are not found in typical applications. This way viruses can be scanned even before their signature is known to the anti virus s/w vendor

⇒ Denial of service Attack: attempt to overload an infra to cause disruption of a service. Attacker fires a large no. of malformed req. Usually one computer alone has insuff. power or bandwidth, distributed DOS attack is used.

Prevention:

- ⇒ split business & public resources
- ⇒ move public facing resources to external cloud providers
- ⇒ setup automatic stability
- ⇒ Lower Time to live of DNS records to reroute traffic to other servers on attack.

Measures on a ddos attack:

- ⇒ Inform ISP & ask for help
- ⇒ Run script to terminate connec^{ns} from same source if >10
- ⇒ Change to an alternative server
- ⇒ Reroute or drop suspected traffic

CDN can take mitigating actions.

⇒ Social engineering: using social skills to manipulate people to obtain info.

⇒ Phishing: email redirecting to seeming legit website asking everything

⇒ Baiting: uses physical media, like USB flash drive, & relies on the curiosity of people to find what is on it.
To mitigate, disable 'auto-run' feature on all org^{n} PCs.

- Security Patterns

→ Identity & Access Management

Process of managing the identity of people & systems, & their permissions. 3 steps:

① Identification: users claim who they are, by providing name
② Authentication: claimed identity is checked, using a password
③ Authorization: Permissions are granted related to identity

* OS does IAM, called Trusted computing Base (TCB)

* Single Sign On (SSO): log in once & authorized to all SSO enabled apps. Typically implemented using identity providing systems like LDAP, Kerberos or Microsoft Active Directory.

* Federated Identity management extends SSO above enterprise level, across organizations. Participating org. ~~ca~~ share identity attributes based on agreed upon standards.

* Authenticatn can be done by: → something you know (Password)
→ ―――― have (~~Credit~~ Bank Card) Phone
→ ―――― are (fingerprint, iris)

→ Segregation of duties & least privilege

* Assign related sensitive tasks to diff people. No single person has total control of system's security mech. System users have lowest level of privileges to perform task.
There must be separate roles: system manager, security m, super user

* Two man policy, control, two system managers must review & approve each other's work.

→ Layered security / Defense-In-Depth strategy

* Implement security measures in various parts of IT infra, instead of one big firewall, & of diff tech.

* Each layer can be integrated with Intrusion Det Sys, detecting breakins.

* More layers introduce uncertainty for hackers (time, number)

* No single pt of failure

* Increases complexity, all layers must be managed

→ Cryptography

Pratice of hiding info. Encryptn: from readable state to apparent random data.
Cipher: pair of algos for encryptn & decryptn.

* Block ciphers & stream ciphers
↳I/P: block of plaintext & a key
EX DES, AES

↳ create arbitrarily long stream of key material, combined with plaintext bit by bit.
⇒ Used when data in transit using a N/W. EX: RC4

* Symmetric key encryption
⇒ key management diff as unique for every 2
⇒ Diff in establishing secure connⁿ fa key. (chicken-egg prob)

* Asymmetric : two diff but mathematically related keys used.
Public : freely distributed

Pete File → Cipher ——→ Encrypted text ——→ Cipher → File
↑ John's public key ↑ John's private key

* very slow process (1k to 10k times), usually used to exchange key for symmetric encryptn.
* also called public key cryptography

Ex: Diffie-Hellman & RSA algo.

* Hash fns & digital signatures:

↳ piece of data as I/P and output a short, fixed length text string unique can be used to validate integrity of data.

Ex: MD5, SHA1, SHA512

↳ Digital sign : ⇒ Text is hashed & encrypted using private key of sender
⇒ Receiver decrypts using sender's public key, then hashes the text and compares with decrypted hash.

~~* Cryptographic attacks~~

- GO LIVE SCENARIOS

Scenarios that can ~~be~~ put new infra in prodn as replacement of an existing system.

→ Big Bang : At a set time, the existing sys is switched off & new sys is immediately put in production, after a short data migrn run
→ riskiest scenario ⇒ may be impossible to roll back to old system
⇒ downtime can occur if something goes wrong during the switchover.

→ Parallel Changeover : Both sys run simultaneously for some time (weeks). Allows testing new system on funcn & NFRs.
⇒ switching back is possible at any time
⇒ cost of maintaing both, extra effort for sync. many designs don't allow ||.

→ Phased changeover : Individual comp / funcnalities taken over one by one.
⇒ Reduces risk, gradual
⇒ Costly ; creating interface b/w old & new sys which can introduce risk

- MONITORING

Inspects IT comp for events like error condns or signs of upcoming failures. Ex: disc with less space, Exc. CPU utilizn, N/w b/w
Monitoring systems ⇒ Nagios, Zabbix, HP Op. Manager, BMC Patrol

- **Simple Network Management Protocol (SNMP)**

SNMP can be used to remotely change or update configuratⁿs & collect stats & performance info of infra comp. Devices that support SNMP: routers/ switches/ servers/ n/k statⁿ printers/racks

→ Uses agent/management model

Man. server collects info from all attached dev, agent resides on monitored device having local knowledge of the system it resides on, & translates that info to SNMP protocol.

→ SNMP protocol allows reading values (at reg. polling int. of 30 sec) to NMS & shown to sys. man. as graphs.

→ SNMP supports traps: an alarm sent to NMS when a value exceed default.

→ security: using shared secret string called community name): provides access to agent functionality

- **Logging**

→ Log data used to correlate events & identify sources of appⁿ issues, to identify trends to predict or prevent unavailability, security vulnerab.

→ Tools to analyze log data: Splunk & Logstash

→ Log analysis for following reasons:

* compliance with security policies
* system troubleshooting
* forensics
* security incident response.

→ Time synch. needed to correlate events.

→ Log analysis moving into Big Data

→ Diff b/w monitoring & log analysis: Log An. is done afterwards, not real time

- **DECOMMISSIONING INFRASTRUCTURES**

At the end of the lifecycle

→ **Preparation**

* Prepare a plan (date)   * Inform in advance
* check for interdep & remove   * determine if & how long backup
* check if system is really not used anymore (ex check firewall logs)
* Ask for vendor assistance   * Inform datacenter floor manager

→ **Execution**

* Create final backup   * remove sys from monitoring & alert sys
* remove from backup sch   * close N/W commⁿs
* switch off (& stand by to redeploy if a dep pops up)
* Physically remove H/w   * Remove cabling & patching

DATACENTER

Most IT infra H/w, except end user devices is hosted in datacenter.
Datacenter provides power supply, cooling & fire prevention, equipment racks.

Datacenter Building Blocks

* Datacenter Categories

→ sub equipment room / patch closet : contain patch panels for connections to wall outlets in offices, & small eq like N/w switches

→ main equipment room: small datacenter in office

→ Org. owned datacenter: main central IT eq

→ multi-tenant datacenter: used by service providers for multiple organzns.

* Datacenter Location

→ Environment : * Enough space to expand the datacenter
* Floods / Hurricane / Earthquake / Fireworks storage / Waste dump / climate / chemical plant
(should be low ambient with low fluctuatns)
* Crime Rate (vandalism) Near Airport (crashes)
* Easily reached in emergencies? Close to maint. staff

→ Utilities : * 2 independent power providers & internet providers?
* cheap power? renewable power? / Enough power? Reliable?
* Cabling routes to the building & inside it determined?
* is present in shared building? How reliable is other users?

→ Foreign Countries : * country reachable at all times?
* corruption? / politically stable? / legal status of data?

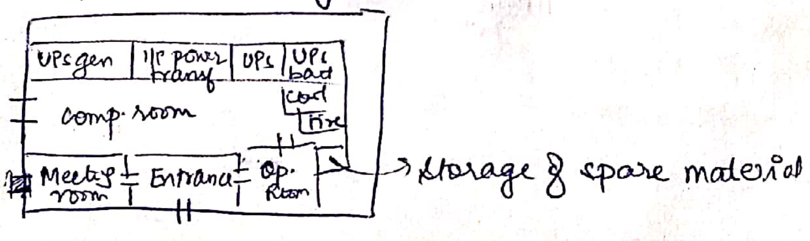
* Physical structure

→ Floor: Must be able to carry 1500 – 2000 kg/m².
* Raised floors: metal frameworks carrying tiles, height 40-120 cm.
Disadvantage:
Expensive, Height decreased, doors & eq loading slopes hard to install
Fire can easily spread

→ walls, windows, ~~floors~~ Doors
walls: Firewall, fire rating
windows: Not desired, if present, should be shatterproof, translucent
Doors: Min 1m x min 2·1 m (eq brought in easily), resist forced entry, fire rating, Emergency exits clearly marked, monitored, alarmed

→ water & Gas Pipes: No leakage

→ Layout:



* Power supply (KW–MW)
calculated in KW/m^2. Normal density datac ⇒ 2–6KW/m^2
High ⇒ 10–20KW/m^2

UPS (Uninterruptible Power supply)

Issues with power supply:
- → Blackout (total loss of power)
- → Surge (A period of High V)
- → Spike (Instant jump)
- → Brownout (voltage drop)
- → waveform issues

UPS provides high quality electrical power in emergency, & filters the power.
UPS installⁿ consists of fillers, diesel power generator, batteries & flywheel sys.

→ Power generators
0·5–2MW Power, Diesel should be refilled regularly, loses calorific value

Testing regularly : → Test working of generator
→ old diesel is used up
→ Use power genⁿ at peak time

→ Battery powered UPS
Batteries last 5-15 minutes, power generator must be started during this period.
3 types –
① Standby UPS/off-line systems : used in small setups, provides AC power from battery using electronic inverter.

② Line Interactive UPS: uses transformer in b/w, works as filter for many power issues, provides AC ______.

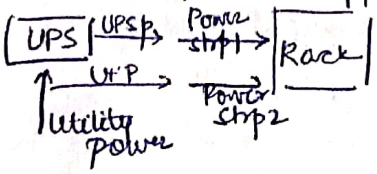
③ Double Conversion UPS: Convert AC to DC, then back to High Qual. AC using an inverter. Hence power to IT systems is local & free of power issues. Provides AC from DC batteries, which eliminates switch over moments & avoids AC power phase changes.

→ Flywheel UPS
Utility grid to motor rotating a flywheel generating electricity
10–20 sec, 50K–55K rotations/minute.

→ UPS maintenance
- → Batteries: Every 3-5 years
- → Flywheel → regular bearing repl, upto 30 yrs.
- → Power generator: preheated, monthly testing

→ Power distributⁿ
2 types of PDUs : → floor mounted
→ power strips, rack PDUs, feed the rack

usually redudancy of 2 power supp in comp, 2 power strips.


UPS
UPS p
Power strip1
Rack
U·P
Power strip2
utility power