Key Security Concepts

09 August 2020 16:27

CIA Triad

Confidentiality
- prevent disclosure of data without prior authentication
- encryption can be used

Integrity
verify data sent/received has not been modified by an unauthorized person
- implement technical controls such as algorithms & hashes
etc. SHA1, MD5, SHA256
hash is an algorithm
- can use websites to generate a hash and also to check a downloaded file hash
- if it's different than it has been tampered with

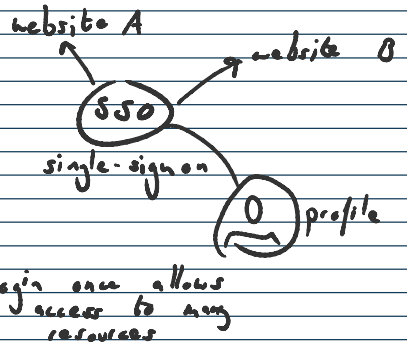
Availability
ensure data is always available when needed
Technical implementations:
- RAIDs
- Clusters
- ISP Redundancy
- Backups

Non-repudiation = valid proof of the ID of the data sender/receiver
- digital signatures
- logs (ie log on sender email client that they sent an email)

Access Management

Access criteria
- groups (management, finance etc..)
- time frame & dates (9-5, Mon-Fri)
- physical location (country, local, city..)
- transaction type (read/write..)

"Need to know" - just information needed



Concepts:
- identity proof
- Kerberos (to implement SSO)
- mutual authentication (secret key)
- SID (security ID)
- DACL (discretionary access control list)
  - you decide who can access your own files

Incidence Response

Managed process to manage and monitor security events and execute response with correct resources

Event: an observed change to the normal behaviour of system
i.e. firewall policy pushed, passwords changed

Event : an observed change to the normal behaviour of system
i.e. firewall policy pushed, passwords changed

Incident : event that negatively effects "CIA" of organization

Response Team : (aka CSIRT) receives security alerts and analyses them

Investigation : determine the circumstances of the incident

key concepts

e-discovery - data inventory, understand tech status, data management etc.
(what is the technical context)

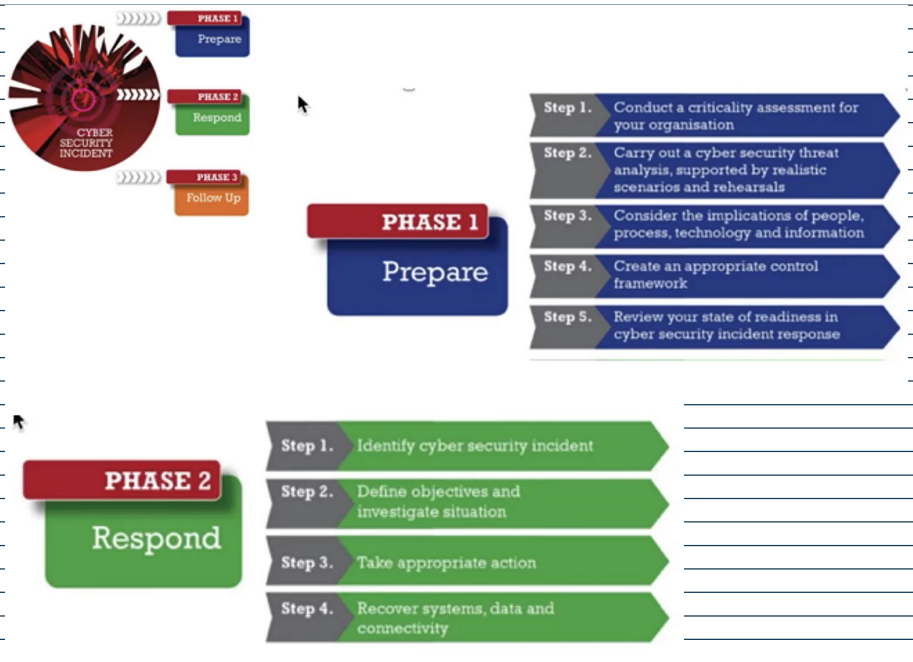
automated systems - technologies to enhance the incident response mechanism
(SIEM, SOA, UBA, big data analysis, AI, honeypots)

BCP & disaster recovery - understand company to prepare for BCP
- what are critical business areas
- what triggers a BCP
- how to restore everything to normal

Post-incident - root-cause analysis
- understand difference between error, problem, isolated incident
- lessons learned

typo / many errors or system crash / one time event - can replicate error?

Process of Incident Response: can check IBM event response cost calculator

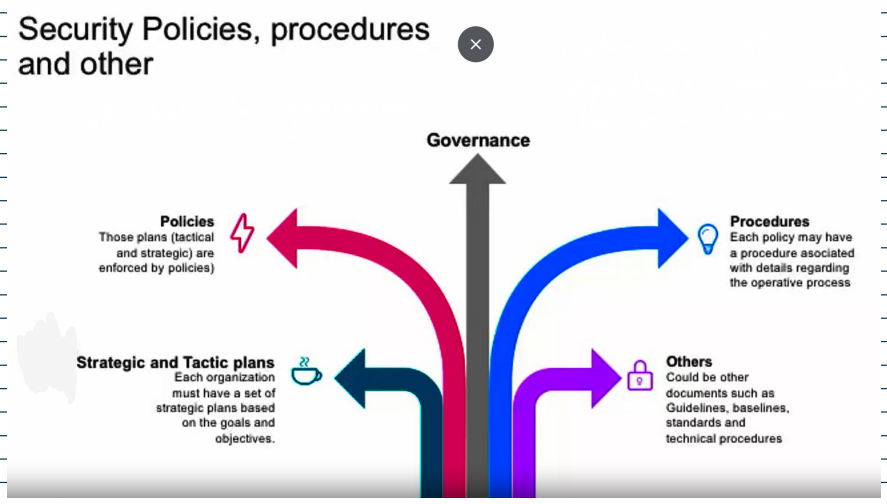


Frameworks and Best Practices

Framework example - COBIT
- Best practices - ITIL
  - to improve controls, methodologies and governance of IT
  - translate business needs into technical needs

Normative & compliance
- specific rules to follow (HIPAA)
- enforced by government & industry

IT Governance Process



Compliance and Audits

Example policies - SOX (financial), HIPPA (healthcare patient privacy), GLBA (finance), PCI/DSS (credit card transactions) (regular pentesting requirements)

Audits - internal/external to ensure compliance with security requirements
- need these in order to obtain above credentials to deal with credit cards, patient data etc...

Penetration Testing Process

Penetration Testing Process

Simulating attack to evaluate computer/network system security

"Ethical hacking" - Mile 2 CPTE Training (how to conduct pentest)

- Footprinting
- Scanning
- Enumeration
- Penetration
  - Denial of Service
  - Elevation of Privilege
- creating backdoors
- covering tracks

OWASP

Test framework

top 10 attacks for web apps and apps

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

The Open Web Application Security Protocol