M T W T F S S
Page No.: YOUVA
Date:

(Wi)

Module - 3 Cybersecurity Compliance Framework & System Administration 13/09/2022

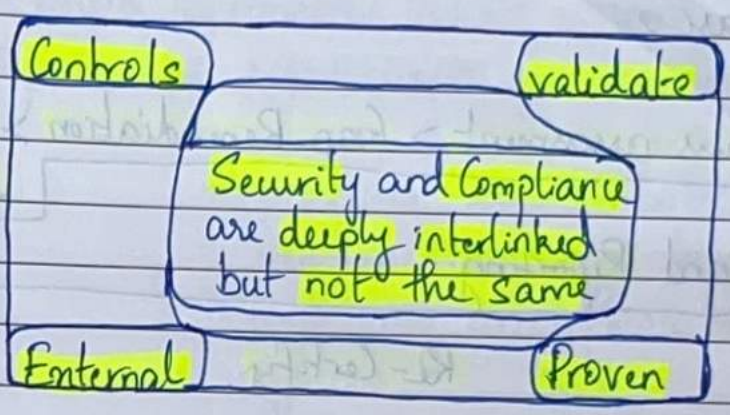
⇒ Security, Privacy and Compliance (related but not same)

↳ Security:
- Designed protection from theft or damage, disruption or misdirection
- Physical controls - for servers in data centers
- Technical controls (log data collection, encryption, etc)
- Operational controls (server configuration, updation, staff training, etc)

↳ Privacy
- how info is used, who that info is shared with, or if that info is used to track users

↳ Compliance
- Tests that security measures are in place
- which and how many depend on specific compliance
- covers business practices, vendor agreements, organisational controls, etc

↳ Compliance checklist



↳ two main categories for compliance

- foundational : General specifications
  : not legaly required
  : ex: SOC, ISO
  ↓ ↓
  Security operations center [international organization for standardization]

- Industry : specific to an industry, dealing with specific data
  : often legal requirements
  : ex: HIPAA, PCI DSS
  ↓ ↓
  Health insurance portability and Accountability Act
  Payment card industry Data Security Standards

M T W T F S S

Page No.: YOUVA

Date:

↳ Typical Compliance prouss

phase 1 phase 2

establish scope > Readiness assessment > Gap Remediation > Testing/ Auditing > Management Assertion and Reporting

Re-Certify.

general prouss for any compliance / audit prouss

⇒ GDPR → General data protection Regulation

↳ european standard that focusses on privacy of european data

- focus on Compliance, Data protection and Personal data.
- 4% or € 20M potential penalty for non-compliance.

⇒ Key terms

Data Subject (→ EU Resident) ⟷ Controller (→ Bank) ⟷ Processor (→ you, if bank is processing your application)

- Data Subject: An identified or identifiable living natural person
- Controller: Determines the purpose and means of processing of personal data
- Processor: processes personal data on behalf of controller

↳ processing: any operation performed on personal data (storage, access)

⇒ ISO (27000) → International Organigation for standardigation

↳ keeps information assets secure
↳ providing requirements for an information security management system (ISMS)
- provides requirements for establishing, implementing, maintaining and continually improving an information security management system.

↳ ISO 270018 - privacy
↳ ISO 270017 - Cloud Security
↳ develops standards not certification.
↳ can get certification following audit by 3rd party accredited certification body.

⇒ SOC Reports

- SOC 1
  - used where systems are being used for financial reporting

- SOC 2
  - addresses service organigation's controls relevent to their operations and compliance.

- SOC 3
  - general use report to provide interested parties with CPA's opinion about same controls in SOC 2

↳ SOC 2 principles

- Security
- Availability
- Confidentiality
- processing integrity
- Privacy

↳ Auditors look for:

- Accuracy → control results assessed for pass/fail
- Completeness → do control implementation cover entire offering
- Timeliness → controls performed on time?
  - with (else)
- Resilience notice → chuk and balance for untimeliness
- Consistency → shifting control implementation raises concerns about above, plus increase testing.

↳ What does SOC1 / SOC2 test

- General controls
- Organization and management
- Communications
- Risk management and design/implementation of controls
- Monitoring of controls
- Logical and physical access controls
- System operations
- Change management
- Availability

⇒ HIPAA

↳ HIPAA Security Rule establishes a set of security standards for protecting certain health information that is held or transferred in electronic form.

↳ protects electronic protected health information (ePHI)

⇒ PCI DSS

- introduced in 2004
- applies to all entities that store, process and/or transmit cardholder data
- covers technical and operational practices for system components
- requires a total of 264 requirements.

↳ Goals

- Build and maintain a secure network
- protect cardholder data
- Maintain vulnerability cardholder data
- Implement Strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy.

↳ PCI requirements

- approved Scanning vendor scans
- use PCI scan policy in Nessus for internal vulnerability scans
- File integrity monitoring (FIM)
- firewall review frequency every 6 months
- Automated logoff of idle session after 15 minutes
- Responsibility Matrix
  ↳ responsibilities of entity providing PCI support and consumer.

Note :

- HIPAA security rule requires covered entities to maintain admin physical and technical safeguards for protecting e-PHI
- HIPAA administrative safeguards include Security personal and workforce Training and management

⇒ Center for Security
Internet

↳ Critical Security Controls

- Basic
- foundational
- Organizational

↳ Implementation Group 1

- An organization with limited resources and cybersecurity expertise available to implement sub-controls.

↳ Implementation Group 2

- An organization with moderate resources " "

↳ Implementation Group 3

- A mature organigation with significant resources " "

M T W T F S S
Page No.:
Date:
YOUVA

W2

⇒ Client

- system/user that accesses resources on a server.

↳ endpoint → remote computing device that communicates back and forth with a network to which it is connected. Ex: phone, Desktop, tablets etc...
devices are front line of attack

↳ Common types of endpoint attack:

- spear phishing - email imitating a trusted source designed to target a specific person or department.
- Watering hole - malware placed on a site frequently visited by an employee or group of employees
- Ad Network attacks - Using ad networks to plan malware onto a machine through ad software
- Island hopping - supply chain infiltration

⇒ 4 Social engineering Threats to prepare for

- Business email Compromise
- Extortion
- Pretexting
- Whaling and Catphish Scams.

M T W T F S S

Page No.: YOUVA

Date:

⇒ Endpoint protection

- endpoint protection management : policy based approach that requires endpoint devices to comply with specific criteria before access to network resources is granted.

- endpoint security management : purchased as software, discover, mange and control computing devices that request access to corporate network.

- endpoint security systems : work on client/server model in which centrally managed server or gateway hosts security program and an accompanying client program is installed on each network device.

↳ Unified endpoint management

→ A UEM platform is one that converges client-based management techniques with mobile device management (MDM) application programming interfaces (APIs)

M T W T F S S

Page No.:	YOUVA
Date:	

Endpoint detection and Response

Key mitigation capabilities for endpoints

- Deployment of devices with network configs
- Automatic quarantine / blocking of non-compliant endpoints
- Ability to patch thousands of endpoints at once.

Endpoint detection and response

- Automatic policy creation for endpoints
- Zero-day OS updating
- Continuous monitoring, patching and enforcement of security policies across endpoints

Examining an endpoint Security Solution

- threat hunting
- detection response
- user response

Unified endpoint management (UEM)

- Devices and things (tabs, phones, laptop, IOTs)
- Apps and Content (Apps, content, data)
- People and identity (identity, threats, connectivity)

↳ client management systems (traditional)

- involves an agent-based approach
- Great for maintenance and support
- Standardized rinse & repeat process
- Applicable for some OS & servers

↳ Mobile device management

- API-based management techniques
- Security and management of corporate mobile assets (documents)
- Specialized for over-the-air configuration
- purpose-built for ~~ph~~ smartphones & tabs

Modern UEM ⇒ Traditional Client management + MDM APIs

⇒ Windows patching

↳ patches: set of changes to computer program or its supporting data designed to update, fix or improve it.
ex: fixing security vulnerabilities, bugfixes.

↳ four types of Updates for windows OSes

- Security updates ①
- Critical updates ② } released immediately post testing
- Software updates ③
- Service packs ④

① → security updates against new and ongoing threats.
→ classified as : Critical, Important, Moderate, Low, or non-rated

⑤ → high priority updated
→ set as automatic

③ → expand features and improve reliability

④ → roll ups or compilation of previous updates to ensure you are up to date on all patches since release of products.

↳ 87% of vulnerabilities found in top 50 programs such as adobeflash and reader, Skype, Java, various media players.
↳ 13% stem from Os and microsoft programs.

M T W T F S S

Page No.: YOUVA

Date:

↳ ~~Patch~~

↳ patching process

- Patch released
  - OS
  - App
- Testing
  - small test group
  - compatibility with custom apps
- Distribute to organization
  - send to broader group
  - patch vulnerabilities

⇒ 7 patch management practices to help protect data

- Use proper discovery service
- Use heterogenous OS platform support
- platform application patching
- Apply coverage on and off premise
- Patch every week
- Be agentless in the data center
- Mitigate after expectations

M T W T F S S

Page No.: YOUVA

Date:

(W3)

14/09/2022

⇒ MS Windows

↳ Windows Acuss Control

- users and groups (Security principals) have assigned rights and perms that inform OS what each user and OS can do.
- Security principals perform actions on objects

↳ privileged accounts

- administrators of window servius have direct or indirect acuss to most or all assets in an IT organization
- admins configure windows to manage acuss control to provide security for multiple roles and users.

↳ local user Accounts : stored locally on windows workstation or server

- Default local user accounts
  - Admin account
  - Guest account
  - Help Assistant account
  - Default Account

- Default local system accounts
  - SYSTEM
  - NETWORK SERVICE
  - LOCAL SERVICE

↳ local users stored in the users folder.
- Security considerations
  - Restrict and protect local accounts with admin rights
  - enforce local account restrictions for remote access
  - Deny network logon to all local admin accounts
  - create unique passwords for local accounts with admin accounts.

↳ Windows security App
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device Security
- Device performance & health
- Family options

M T W T F S S
Page No.:
Date:
YOUVA

↳ Active Directory

- Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information easy for administrators and users to find and use.
- eg: network folders, network printers.
- Objects typically include shared resources such as servers, volumes, printers, and the network users and computer accounts.
- security is integrated with AD through authentication and access control to objects in the directory via policy-based administration.

↳ Active Directory Accounts

- Default local accounts in A.D
  - admin account
  - Guest account
  - HelpAssistant account
  - KRBTGT Account
- settings for default accounts in A.D
- manage default local accounts in A.D
- secure and manage domain controllers.
  - ↳
    - seperate admin accounts from user accounts (1)
    - create dedicated workstation hosts without internet and email access (2)
    - Restrict admin logon access to servers and workstations (3)
    - Disable account delegation right for admin accounts (4)

(1) ideal → create multiple, seperate accounts for an administrator who has a variety of job responsibilities that require different trust levels.

② Ideal → Rustrict workstations from having any network connectivity, except for the domain controllers and servers that the admin acounts are used to manage.

③ Ideal - Rustrict server admins from signing in to workstations in addition to domain admins.

④ best practice to configure user objects for all sensitive acounts in A.D by selecting "Account is sensitive and cannot be delegated" check box under "Acount options" to prevent acounts from being delegated.

↳ Active Directory groups

- Security groups are used to collect user acounts, computer acounts and other groups into manageable units.

↳ 2 types of administrative responsibilities
- Service admins
- Data admins

↳ 2 types of groups in A.D
- distribution groups - used to create email distribution lists.
- Security groups - used to assign perms to shared resource

↳ Group Scope - Universal
- Global
- Domain local

↳ Admin Centera - locally developed, browser based management tool set that lets you manage windows servers with no cloud dependency.

To summarize

⇒ Active Directory is a directory service developed by microsoft for windows domain networks. Included in most windows Server OSs as a set of processes and services.

provides centralized adminstration of an entire network from a single computer called server.

↳ Kerberos Authentication → most AD systems leverage this as auth protocol.

- Kerberos is an authentication protocol that is used to verify identity of a user or host.
- predominant mechanism which is used within windows for authentication and for securing A.D environment.
- Benifits :
  - Delegated authentication
  - SSO (Single-Sign on)
  - Interoperability (if authenticated to AD, then resources within AD also authenticated)

- more efficient authentication to servers
- mutual authentication

↳ Windows Server logs

- records of events that happen on your computer, either by person or running process
- they exist to track what happened, to troubleshoot problems, investigate security events

- Windows event log
  - contains logs from OS and other application.
  - some apps log in text format (easy to analyze)

- Windows event viewer
  - displays event logs in windows event viewer
  - lets you navigate, search and filter particular types of logs, export for analysis, etc

↳ Auditing windows server

↳ nine events one can audit

- Account Logon events – shows each instance of user logging on to or logging off from another computer in which this computer is used to validate

- Account management – someone has changed account name, enabled or disabled account,

created or deleted account, changed password or user group

- Directory service access – someone accesses an AD directory service client that has its own system access control list (SACL)
- logon events - someone has logged on or off your computer.
- Object access - someone has used a file, folder, printer or other object. Also can audit registry keys. (not recommended)
- Policy change - attempts to change local security policies and if user agreements, auditing policies or trust policies have been changed.
- Privilege use - someone performs a user right
- process tracking - events such as program activation or program exiting occur.
- System events - someone shut down or restarted the computer or when process or program tries to do something that it doesn't have perms to do.

⇒ Linux

- Kernel
- Shell → interface to Kernel

↳ Run levels

- To run any run level in terminal

> init 6

this run level is for reboot. (hence reboots the system)

↳ Linux Commands

> shutdown -h now (shuts down immediately)
> shutdown -h +10 (shuts down after 10 mins)
> shutdown -r now (system reeboot)
> shutdown -fr now (force filesystem chek during reboot)

> ps -efH | more (view current processes in hy structure)
(H stands for procss heirarchy)

> free -g (displays free, used, swap memory in system)
(-g to display in GB)

> top (top processes running)

> mkdir -p dir1/dir2/dir3/dir4/ (creating nested directories)

> ifconfig -a (view all interfaces along with status

> ifconfig eth0 up (To start or stop a specific interface)
> ifconfig eth0 down

M T W T F S S

Page No.:

Date:

YOUVA

⇒ Samba

- provides seamless file and print services.
- uses TCP/IP protocol installed on host server.
- also allows host to interact with microsoft windows client or server.
- allows interoperability between Linux/Unix servers and windows based clients

> sudo apt-get install samba samba-common python-glade2 system-config-samba.

÷ configure samba, edit file at /etc/samba/smb.conf

> nano smb.conf

> [anonymous]
path = /samba/anonymous
Browsable = yes
writable = yes
guest ok = yes
read only = no
force user = nobody

- Then create directory,

> mkdir -p /samba/anonymous

- set perms

> chmod -R 755 /samba/anonymous
> chown -R nobody:nogroup /samba/anonymous

- restart samba to apply new config

> service smbd restart

↳ Now go to windows host, we can acess linux in windows by entering IP of linux in windows search field of menu or use network browser of windows file explorer to connect to share

-> Network > 192.168.1.8 (ip of linux machine)

- we see a file named anonymous in here
- edit the folder file and add the following info

↳ Secure Samba folder

- for a password-protected share, create a group called "smbgrp" and user to acess samba server:

> addgroup smbgroup
> useradd smbadm -G smbgrp
> smbpasswd -a smbadm
> root@jith:/samba/anonymous# smbpasswd -a smbadm
> NEW SMB password:
> Retype new SMB password:
> Added user smbadm.

- create the folder with name "secured" in /samba folder and give it perms like this:

> mkdir -p /samba/secured
> cd /samba

>chmod -R 770 secured
>chown root:smbgrp secured

- edit samba config file and add these files

>nano /etc/samba/smb.conf
>[secured]
path = /samba/secured
valid users = @smbgrp
guest ok = no
writable = yes
browsable = yes
>service smbd restart

↳ In windows open "ip" network device again, it will request a username and password now.

W4

⇒ Cryptography

- Missing and faulty crypto consistently appears on OWASP Top 10 list
  - Sensitive data exposure

↳ ⇒ cryptographic failures Example attack Scenarios

- An application encrypts credit card numbers in a database using automatic database encryption. However, data is automatically decrypted when retrieved, allowing SQL injection flaw to retrieve credit card numbers in clear text.

- password database uses unsalted or simple hashes to store everyone's passwords. A file upload vulnerability allows attacker to retrieve the password database. All the unsalted hashes can be exposed with a rainbow table of pre-calculated hashes. Hashes generated by simple or fast hash functions maybe cracked by GPUs, even if they're salted.

- site not using TLS - downgrade HTTPS to HTTP - steal users session cookie - replay cookie - access or modify user data.

↳ encryption : process of encoding data in a way that only authorized party can access it
: provides confidentiality, but not integrity.
: can be encrypted - at rest, in use and in transit

Hash function

- provides integrity, not confidentiality
- eg: MD5, SHA-1, SHA-2, SHA-3
- used for integrity checking and sensitive data storage.

Digital Signature

- mathematical scheme for verifying authenticity of digital messages and documents
  - Uses hashing and public key encryption
  - ensures authentication, non-repudiation, and integrity

↳ encrypt all sensitive data you aren't handling (and also ensure its integrity) - (missing encryption of data and communications)

↳ you have to assume that the files containing sensitive information may be exposed and analyzed. - (" ")

↳ rely on proven cryptography that was scrutinized by thousands of mathematicians and cryptographers. ← (Implementing your own cryptography)

↳ - (Relying on Algos being secret)
Always assume that your algos will be known to the adversary

↳ Rely on hard to guess, randomely generated keys and password that are stored securely. -(using hardcoded/predictable weak keys)

↳ -(ignoring Encryption export regulation rules)

↳ Encryption of Data

- Encrypting data at rest (files, config files, db, backups)
- some algos outdated and no longer secure
  eg:- DES, RC4, etc
- Using hard coded/easily guessed/insufficiently random keys. eg:- do not reuse keys
- storing keys in clear text in proximity to data they protect.
  -store keys in secure keystores
- Using initialization vectors (IVs) incorrectly
  -use random IV everytime
- preferable to select biggest key size.
- Consider Homomorphic encryption if it can be applied to your application.

  ↓
  class of algo which allow you to operate on data without decrypting it.

↳ encrypting data in transit

- no communication in cleartext
- TLS/SSL - commonly used protocol.
  ↓ ↳ transport layer security
  secure socket layer

-pitfalls
- Using self signed certificates
- accepting arbitrary certificates
- not using certificate pinning (check against set of expected certificates)
- using outdated protocols
  - ex: DROWN, POODLE, BEAST, CRIME BREACH)
- nessus, sslscan - reviews TLS
- Allows TLS downgrade
- not safeguarding private keys

-Recommendations
- implement forward secrecy
- do not use compression under TLS (leads to sensitive exposure)
- implement HTTP strict transport security (HSTS)
- stay informed of latest security news)

↳ Hashing
- Use SHA-2 (SHA-256, SHA-384, SHA-512, etc) and SHA-3
- MD-5 and SHA-1 should NOT BE USED.

-Piffalls
- using predictable plaintext
- To solve above problem, use salted hashes when validating passwords.

-Additional recommendations

- Use key stretching functions (~~PBK~~ PBKDF2) with large no. of iterations.
- eg:- PBKDF2 using SHA256 and 100,003 iterations.
- slows down the calculation of hash and hence bruteforcing is impossible.

↳ Message Authentication codes (MACs)

- confirm that data block came from stated sender and hasn't been changed.
- Hash based MACs - (HMAC-256, HMAC-SHA3)
  - ↳ generated with secret key
- HMACs help when data may be maliciously altered while under temporary attacker's control (eg:- cookies, transmitted messages)
- Even encrypted data should be protected by HMACs. (avoids bit-flipping attack)
  - ↳ changing bits and altering messages

↳ Digital signatures

→ verify integrity of
- data exchanged between nodes in the product
- code transmitted over network for execution at client side (eg:- JS)
- data temporarily saved to customer machine (eg:- backups)

M T W T F S S
Page No.:
Date:
YOUVA

↳ Safeguarding Encryption keys

- store in secure cryptographic storage
  eg: keystores
- In Java, you can use Java KeyStore (JKS)
- To store key encryption keys;
  - use hardware secure modules
  - use Virtual HSM
  - Derive KEK from
    - user-entered password
    - data unique to machine product is running on (eg: Timestamps, filenames)

↳ Quatum computing is using quantum-mechanical phenomena may negatively affect current crypto algos.

⇒ Common weakness enumeration (CWE) Top 25 most dangerous software weaknesses can be found at

cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

⇒ To summarize

- Encrypt all sensitive data
- Rely on proven Algorithms and use them correctly
- Do not write your own Algos or rely on them being hidden
- Use hard-to-guess keys and store them securely.