Chapter 9

Thursday, August 24, 2023 11:38 AM

physical controls = protect access to secure areas

redundancy and fault tolerance = remove single points of failure

backups = make sure data can be recovered

Comparing Physical Security Controls

Perimeter - fences around perimeter
guards + barricades

Buildings - guards, locked doors, lighting, video cams

Secure work areas - restrict access to certain areas of the building

Server rooms - only certain IT have access
additional controls like locks inside

hardware - locking cables for individual systems
safes

[illegible] **camoflage** - hide buildings

industrial camouflage - hide buildings or parts of buildings

greenery

Securing Door Access with Cards

proximity cards - credit-card sized cards that activate when close to card reader

used common for entrance to building

smart cards can also include prox card electronics

or just enter into smart card reader

these accept power from reader

can combine w/ PIN to have MFA

have + know

Comparing Locks

door access system - only opens after

door access system - only opens

access control mechanism

physical, elec, bio, cable locks

want to limit # of access points

need to consider fire/emergency

Physical Locks

simple, cheap

Physical Cipher Locks

4/5 buttons w/ #'s for code

elec / manual

manual requires turn handle after code

could also require pressing multiple buttons at once

dont id users

open to shoulder surfing

Biometric locks

one benefit is they offer id and auth

who entered and when

needs low false acceptance

Cable locks

good theft deterrent for mobile pc

secures pc to piece of furniture

4-digit combo

good for pc labs

Increasing security with Personnel

guards can check IDs or other ACL

deter tailgaiting by monitor prox card use

reception desk/area works as well

robot sentries

typically military but less armed versions for homes

mobile versions for data centers

two-person integrity - requires two auth individuals to perform tasks

NIST only requires for handling of COMSEC keying material - comms security; keying = mats to encrypt/decrypt classified docs

Monitoring Areas with Cameras

areas outside building, entries, exits...

also for high-sec areas like server room

Closed-circuit tv CCTV - transmits signals from cams to monitors

visible proof of person's location

most reliable proof of person's location and activity

smart cards can be stolen

compensating control

ex: smart cards take long time to implement

motion/object detection

Sensors

use to detect changes in env

Common uses

- **motion detection**

  auto, light dimmers, and motion to save on elec costs

  alarms

- **noise detection**

  detect when noise exceeds certain level

  alarms

level

control lights/alarms

- temperature

  heating, ventilation, and air conditioning HVAC have temp/humid sensors

  might also be w/ fire detect

- moisture detection

  detect flood

  turn on water pumps

  turn off systems

- proximity reader

  prox cards sensors

- cards

  smart card/ badge sensors

Fencing, Lighting, and Alarms

and property

fences = barrier around property
control access via gates

dual gates - provide access to "caged" area that requires 2nd code check

lights = deter attackers from entering need to protect so they cannot turned off

alarms
fire, unauth access

motion detection can be integrated into all 3

infrared = more advanced temp sensor

Securing Access with Barricades
fences not enough

fences not enough

barricades to deter vehicles

bollards - short vertical posts made of concrete/steel

best for preventing vehicles from ramming

Using Signage

"Auth personnel only"

deterrent

Drones

small flying vehicles

unmanned aerial vehicles UAVs

most have cams

remote control or onboard pc

good:

can be used as aerial view of area

observe threats

observe

bad: attackers can do

Asset Management

tracking valuable assets throughout their lifecycles

ex: track hardware

asset management reduces

- Architecture and design weakness

purchases go through approval

unapproved assets weaken security through unmanaged resources

- System sprawl and undocumented assets

asset management helps prevent unneeded systems

many orgs use auto methods for

many orgs use ...
inv control

RFID can track devices

helps detect shadow IT

Implementing Diversity

defense in depth - implement several layers of protection

diversity - using diff vendors, tech, and controls

- vendor - implement controls from diff vendors

  ex: two firewalls, one from each vendor

- technology - use diff tech to protect env

  ex: use bio, CCTV, and limit access points to server room

- control - use different control types

Creating Secure Areas

physical security measures

Air Gap

pc or net is physically isolated from another

ensure they are never connected

Vaults

Room or large compartment to store valuables

DoD uses sensitive compartmented info facilities SCIF - rooms in building to process classified info

Faraday Cage

a room that prevents radio frequency RF from entering or

frequency RF

leaving

lightning protection

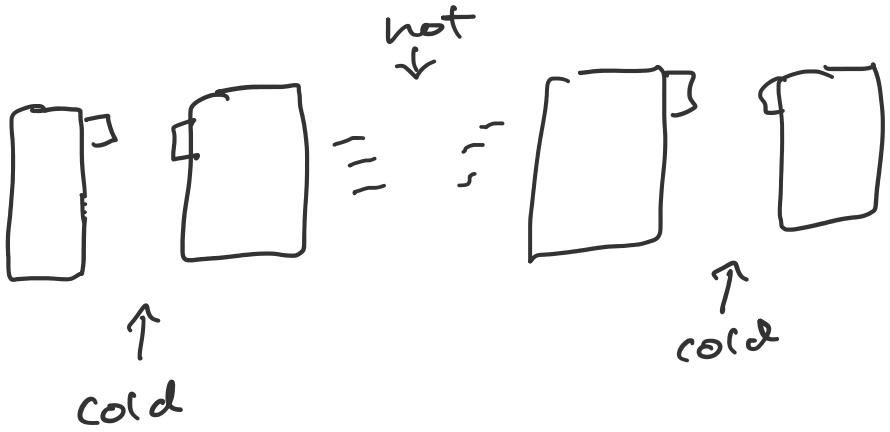
Safes

prevent theft of smaller devices

Hot and Cold Aisles

help regulate cooling in data centers

back of all cabinets in a row faces the back of all in adjacent row



cool air pumped in w/ perforated floor tiles

Attacks

Physical Attacks

- can use smaller devices to seem normal
- install malware
- steal credit card

Malicious Universal Serial Bus Cable

malicious USB cable - has embedded wifi controller capable of receiving commands from nearby wireless devices

pc detects as human interface device HID, so like a keyboard

attacker can issue pc commands w/out logging in

pen testers use USB ninja cable - delivers malware when wireless signal delivers it

Malicious Flash Drive

Malicious Flash Drive

includes malware set to infect pc when plugged in

Card skimming and card cloning

card skimming - capture credit card data at point of sale

ex: on ATMs/gas

card cloning - making copy of credit card using data captured

much harder to do with chips

Fire Suppression

fire extinguishers and fixed systems

- **remove the heat**
  water/ chemicals
- **remove oxygen**
  gas like CO_2: electrical fires
- **remove the fuel**
- **interrupt reaction**

- remove the
- disrupt chain reaction
  w/ cleans

Protected Cable Distribution

where and how you route cables

Attackers can cut cables, attach RJ-45 connector to each end, and connect back with an adapter can use to capture all net traffic

can run cables through cable troughs or wiring ducts

large metal containers or false ceilings

need to keep away from electromagnetic interference EMI sources

Adding Redundancy and Fault Tolerance

adds application to

Adding redundancy

redundancy adds duplication to critical system components and provides fault tolerance

redundancies

- Disk redundancies w/ RAID
- NIC redundancy w/ NIC teaming
- Server w/ load balancers
- Power w/ generators & UPS
- Site w/ hot, cold, warm

Single Point of Failure

component that can cause entire system to fail

Disk

if system uses single disk, it will crash

RAID provides fault tolerance for hard drives

hard drives

server

failure will halt service

load balancing

Power

UPS and gens

Personnel

only 2 person can perform tasks

Business continuity plans help

mitigate

Disk Redundancies

any system has

- processor
- memory
- disk
- Network interface

most susceptible

Disk is slowest and most susceptible

even if disk fails, RAID can tolerate failure

RAID-0

Striping

does not provide any fault tolerance or redundancy

2 or more physical disks that files are spread across

faster read/write because data can be read from all drives at same time

RAID-1

mirroring

uses 2 disks

data written to 1 is written to other

data
to other

you can add another disk controller
so each disk has one

disk duplexing

RAID-2, 3, 4 are rarely used

RAID-5 and RAID-6

RAID-5 = 3 or more disks striped
together

equivalent of 1 disk has parity
info that is striped across
all, providing fault tolerance

if 1 disk fails, disk subsystem
can read remaining drive's
info to recreate original
data

if 2 drives fail data is lost

if 2 drives fail dat-

RAID-6

extension of RAID 5

uses additional parity block and disk

will continue if 2 disk fail

min of 4 disks needed

RAID-10

combines mirroring (RAID-1) and striping (0)

1 + 0 = 10

Variation = RAID-01

RAID-10 min drives = 4

adding more you add

RAID ...

when adding more you add doubles

2, 4, 6 ...

RAID-0

3 500Gb = 1,500 GB

RAID-1

2 500 GB = 500 GB

RAID-10

4 500 GB = 1TB

Disk Multipath

multipath I/O - uses separate data transfer path to and from storage hardware

I can fail but if both I/Os better performance

I can fail
are up it's better performance

Not simple

Storage Area Network SAN to implement

expensive + complex

Server Redundancy and High Availability

high availability - system or service that needs to remain operational with almost 0 downtime

five nines = 99.999%

26 minutes of downtime a year

high capacity load balancers ensure service is always available

active/active Load balancers

Active/active Load balancers

optimize and distribute data loads across multiple pc or net

ex: high traffic site can use multiple servers hosting same site in a web farm

hardware or software

hardware-based - uses factors like processor utilization and # of connections to balance

software-based - uses software running on each to balance

load balances can use round robin or detect which server has least for scheduling

least for scheduling

can also do source address affinity - session persistance

directs user's IP for entire session to certain server

software-based has 1 IP that all requests get sent to then distributes to private server IP

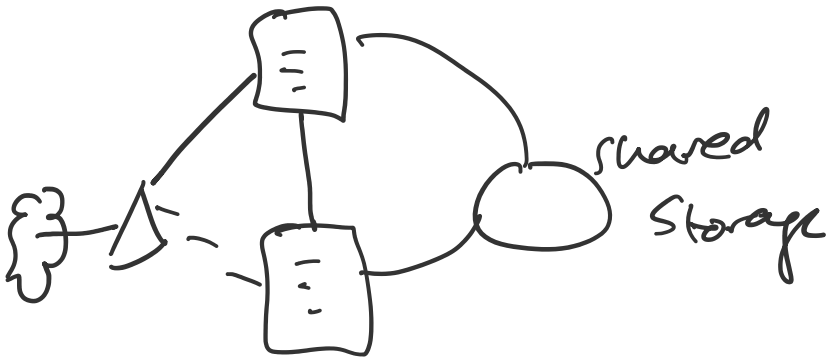
virtual IP

load balancers detect when a server fails

Active/Passive Load Balancers

one server is active, other is not

if one fails, other starts



NIC Teaming

group 2 or more physical net adapters into single software-based net adapter

uses load-balancing

any failures are removed from team

Power Redundancies

uninteroptable power supplies UPS

short-term power and protect against power fluctuation

Dual Supply

redundant power supply

second power if first fails

don't turning off

hot-swap = change w/out turning off

Generators

long term power for outages

Managed power distribution units PDU

common for server racks

distribute power like power strip

provides monitoring for admins

Protecting Data with Backups

copies of data

last corrective control to ransomware

redundancy ≠ backup

ex: RAID-1 or RAID-10

if server is destroyed then all data lost

Backup Media

tape - most common media for backups

stores more data & cheap

disk

much quicker than tape

more expensive

servers / USB

Network-attached storage NAS

dedicated pc for file storage

accessible on net

mult drives + Linux

access/copy files

Storage area network SAN

block-level data storage via a full-net

use for high-speed access to

use for high-speed access to disk/tape

real-time replication of data

SAN requires dedicated hardware with diff protocols

NAS uses standard TCP/IP

Cloud

Online versus Offline Backups

offline

- tapes
- disks
- drives in NAS
- backup targets in SAN

\+ easy/fast access

\+ more control

\- can fail/destroy/stolen

Online = cloud

+ access via internet
+ even if destroyed, always available
+ auto-encrypt

hot-backup - backs up when operational

Cloud - "online"

cold-backup - backs up when offline

"offline" or local

Comparing Backup Types

. full backup
. differential backup - backup all data that has changed since

- differential
  data that has changed since last full backup

- incremental backup - backup all since last full or incremental

- Snapshot and image backup - captures data at a point in time

Full Backups

back up all data

rare to do daily

- time
  can take several hours

- money
  doing full backups requires more media

incremental / differential start w/ full backup

full backup

Restoring a Full Backup

easiest and quickest to restore

only need to restore single full backup

Differential Backups

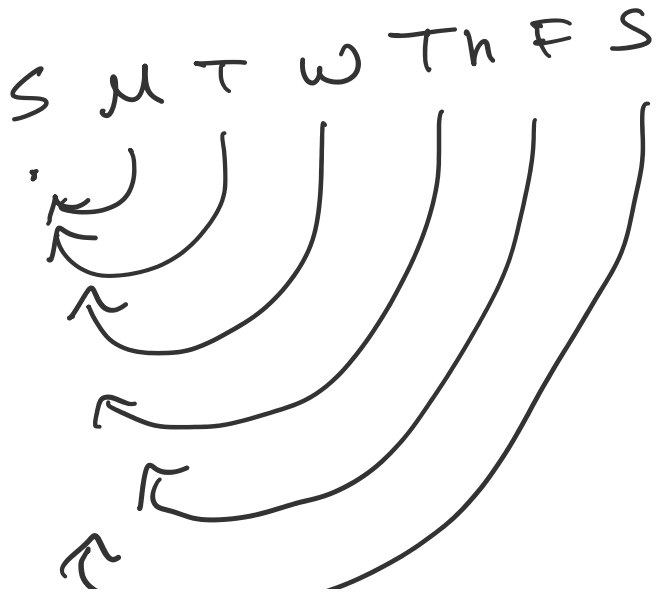
backup changes since last full

ex:

full/differential

full on Sunday

diff on each day till Sunday



diff grows in size each day

Order of Restoration for a Full/Differential Backup Set

ex: store each backup on diff tapes

if sys crashes, which to restore?

- full backup
- latest diff

Incremental Backups

backup data either since last full or incremental

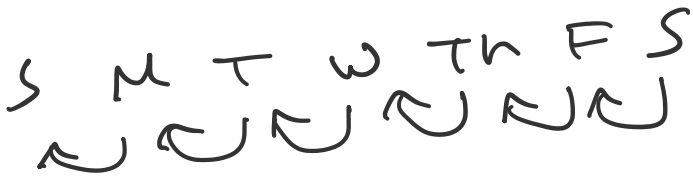
ex:

full/incremental

full on Sunday

- last day on each

Backup to last day or each day



Backups stay about same size

Order of Restoration for a Full/incremental Backup set

full and each incremental needs to be restored in order

full = fastest recovery time w/ money

full/incremental = reduce time to backup

full/differential = reduce time to restore

Choosing Full/Incremental or

Choosing Full/Incremental/Full/Differential

min time required to backup during week = incremental

min recovery time = diff

Snapshot and Image Backups

commonly used with VMs

Copy Backup

copies files to backup media

important to know that malware will try to infect all drives connected to pc

local, USB, NAS

Testing Backups

validate that backups are actually working with test restore -

working with test restore

restoring data from backup and verify

also help w/ getting used to procedure for real crisis

restore data to diff location than original source

Backups and Geographical Considerations

backup policy - what to backup, how often, how to test, how long to retain

geographical considerations

- off-site storages

at least 1 copy stored off-site for natural disaster

- Distance
  decide if close or far away
- Location selection
  depends on environmental issues
- Legal implications
  Backups of PII/PHI
  need to be protected
- Data sovereignty
  data subject to country's
  laws

Comparing Business Continuity Elements

helps predict/plan for outages
of critical functions

business continuity plan BCP

- environmental

- person-made
- internal vs external

Business Impact Analysis Concepts

BIA

part of BCP

id critical sys and components essential to org success

mission-essential functions - must continue shortly after disaster

id vulnerable business processes that support mission essential

BIA Questions

- What are critical functions
- Are there dependencies for critical systems
- What is max downtime
- are most

- What is mos
- What scenarios are most likely to impact
- What is the potential loss from these scenarios

Site Risk Assessment

focused assessment of specific location/site

nat disasters, protecting certain sys,

...

Impact

- loss of life
- loss of prop
- min risk to personnel
- reduce safety for personnel/prop
- What are financial losses

- what are
- rep losses

Recovery Time Objective

RTO - max amount of time to restore system

BIA esfablisu for mission essential

Recovery Point objective

RPO - point in time where data loss is acceptable

ex: server w/ archived data that has changes once a week

want to restore at least last week's data

RPO = 1 week

+ data

RPO

for highly important data any loss may be unacceptable

amount of data you can afford to lose

Comparing MTBF and MTTR

mean time between failures MTBF

higher = more reliable

mean time to repair MTTR

often specified in contracts

Continuity of Operations Planning

COOP - restoring mission-essential functions at a recovery site after outage

office

after orig

ex: hurricane at main office
continue at alt site

failover - move mission essentials to alt site

Site Resiliency

recovery site - alt processing site used for site res

hot, cold, warm

mobile and mirrored

Hot Site

operational 24/7

quick takeover

... software, comms

all equipment, software, comms and up to date data

common to be another active business location

not always instant take over

most effective and expensive

Cold site

really only needs electricity

org brings equip, software, ... when activated

easiest to maintain, hardest to test

Site

but

Warm Site

ex: keep all hardware ... but not use or to date data

Site Variations

mobile - self-contained transport unit

ex: trailer

only needs power

Mirrored - identical to main site and running 100%

realtime transfers to send mods from main site

always up and operational

Restoration Order

primary site first

return least critical functions first because critical are operational

first because
on alt

Disaster Recovery

DRP - how to recover crit sys and data after disaster

use BIA to identify crit sys

can have mult DRP in BCP
ex: 1 for each crit sys

Needs to prio sys to recover

Different phases of DRP

- Activate the DRP
- Implement contingencies
  - implement alt site
  - retrieve off-site backups
  - recover critical systems
  - list

- Recover critical syst
  recover using prio list
- test recovered systems
  use baselines
- after action report

Testing Plans with exercises

- Validate plan works
- test redundancies/backups

tabletop exercise

desktop exercise

discussion-based

coordinator leads group and leads through hypothetical scenario

walk throughs

workshops/seminars to train
[illegible] on their responsibilities

workstation team on their net

Simulations

functional plans to test plans in simulated env

Assessment Notes

1. CCTV can be installed as compensating control
2. Cable locks good to stop theft
3. Air gap is best to make sure net is not accessible to other
4. Secure access to data center
   - Biometrics
   - Access control vestibule
   - CCTV
5. Raid-6 = 2 Drive failure

5. Raid-6 = 2 Drive failure

0 = 0

1 = 1

5 = 1

6. Disk Multipath = fault tolerance that gives more than 1 path for system to data storge system redundancy for data severs

7. NIC teaming for extra bandwidth

SAN helps w/ disk performance

8. Persistence = maintain connection of IP through session

9. Active/passive = Resillience

- backups to

9. Activity

10. full/diff = 2 backups to restore

11. full backups = ransomware resil

12. Mission-essential functions = processes that cause $ loss if fail

critical systems support mission-essential

13. BIA = doc past financial losses

14. RTO = max downtime

15. Tabletop exercises = meet w/ team and practice discussion

w/ team and
scenario through discussion