Chapter 11

Friday, September 1, 2023 12:23 PM

Exploring Security Policies

Security policies - written docs that lay out sec plan in company

admin control

brief, high-level, statements that id goals based on orgs overall beliefs and principles

plans and procedures support policies

policy implement

Personnel Policies

personnel behavior, expectations, consequences

Acceptable Use Policy

purpose of net, how users can

purpose of pc/net, how users can
access, responsibilities of users

may notify that org monitors
usage

also what pc activities user
can consider private

privacy policy - clarifies expectation
of privacy when using org's pc

require to sign AUP + sec training

Mandatory Vacations

help detect when employees are involved
in malicious activity

ex: embezzlement or fiscal activity
need to be present to manipulate
records and respond to inquiries

deterrent

Separation of Duties

principle that prevents any single person from being able to do all functions of critical activity

principle of least privilege + account audits

Least Privilege

grant only privileges needed to perform assigned tasks or functions

services should have <u>own</u> accounts

Job Rotation

has employees rotate through diff jobs to learn processes and procedures in each job

prevent or expose dangerous shortcuts or fraud

w/ <u>only</u> separation of duties, people

w/ only separate

can collude w/ each other

job rotation prevents this

Clean Desk Space

keep desk free of papers

ensure protect of sens data

data theft

Background Check

investigate employee's histories

criminal activity + driving records

check online activity

financial history

Onboarding

granting individuals access to

org's computing resources after

being hired

being hired

principle of least privilege

Offboarding

remove access when leave org

- disable/delete user acc
- collect equip

remove access during exit interview

Non-disclosure Agreement

NDA - between 2 entities to ensure proprietary data is not disclosed

Social Media Analysis

may monitor during employment as well

NDA specify what emp

AUP usually specify what emp can/can't share on social media

can search for org to monitor or search based on specific employee

Third-Party Risk Management

3rd party often introduce risks to be managed

Supply Chain and vendors

best to limit access to vendors have to internal net or data

vendor management system

feedback from vendors such as order status best from web app w/ creds

app w/ creds

vendor diversity

vendor management includes

- limit system integration
- when vendor support stops

EOL + EOSL

↓ dont sell

↓ dont support

Third-Party Agreements

Service level agreement SLA - agree between 2 orgs that stipulates performance expectations

min/max downtimes

ex: ISP w/ org

monetary penalty if 3rd party doesn't provide

MOU

provide

memorandum of understanding MOU

or of agreement MOA

express understanding between 2 orgs
indicating intention to work
tgther for common goal

Less formal than SLA

Business Partner Agreement BPA

details relationship between
business partners

- shares of profits/losses
- responsibilities to each other
- what to do if partner leaves

helps settle conflicts

Terms of Agreement

period that an agreement will be
in effect

Measurement Systems Analysis

Measurement Systems Analysis

MSA - evaluates processes and tools used to make measurements

id variations in measurement process that can result in invalid results

ex: org takes emp temp when walking in

MSA evaluates acc of thermometer by verifying consistent results

Incident Response Policies

IR policies help identify and respond to incidents

security incident - adverse event or series of events that can negatively affect CIA of data or sys

incident

or sys

data breach - security incident where unauth entities access data

Incident Response Plan

formal, coord, plan that personnel can use when responding to incident

Common elements

- Definitions of incident types
  id diff between event and incident
  group into cats like
    - attacks
    - malwar
    - data breach

- incident response team
  team of emp from different areas of exp
    - incident response team CIRT

Computer incident response team CIRT

or SIRT

- how to validate incident
- collect evidence
- protect evidence

- roles and responsibilities

id specific roles for IR team and their responsibilities

Communication Plan

part of IR plan

provides direction on how to comm issues related to incident

common elements

- first responders

ex: help-desk tech

know when to inform IR entities of incident and who to contact

- internal communication

  know when to inform senior personnel of incident

- reporting requirements

  need to report to law or other external entities

  notify consumers if data exposed

- external communication

  who can talk to external entities like media

- law enforcement

  can provide help after an incident

  increase chance of public notice

- customes communication

  when org must noti customers

Data Breach Responses

data loss result

Data Breach Response

IP or customer data loss result in significant monetary loss

most likely that all data breaches are reported to C-level

need to id extent of loss

Stakeholder Management

creating and maintaining positive relation w/ stakeholders

Incident Response Process

common phases of IR process

- preparation

  guidance on how to respond to an incident

  establish/maintain IR plan/procedure

  ex: implement sec controls

- identification

  incidents vs false +

- Identification
  verify incidents vs false +

- containment
  isolate or contain
  protect crit sys while maintain ops
  quarantine or remove device
  modify ACL to isolate net

- Eradication
  remove components of attack

- Recovery
  return all affected sys to normal
  op

- Lessons learned
  valuable lessons used to modify
  procedures

Understanding SOAR

use to respond to low-level sec
events auto

activity

event

Detect + respond to sus activity

use playbooks and runbooks

Playbooks

document formal procedures to follow for well known incidents

steps to take in response to action

Runbooks

implement guidelines documented in playbooks using tools in org

auto respond to incidents or at least assign to admin to investigate

Understanding Digital Forensics

collect info after incident

collect/analyze evidence to crime

collect / analyze evidence to prosecute crime

make sure evidence is controlled and not modified during collection or analysis of data

Computer forensics - analyse evidence from pc to gather details of computer incidents

key aspects of Digital Forensics

important if any evidence collected

Admissibility of Documentation and Evidence

follow specific procedures to ensure evidence is admissible in court of law

maintain an altered original copy of evidence

non-rep - proof individuals were

non-rep - proof individuals
involved

Tags

after item is id as possible evidence, needs to be tagged

formal doc or sticker

date, time, and name of person placing tag on item

control # for chain of custody

Chain of Custody

process that provides assurance that evidence has been controlled and appropriately handled after collection

Chain of custody form - record of every person who was in possession of physical asset

possession of it

who had custody + where

Legal Hold

court order to maintain diff typer of data as evidence

ex: make org maintain digital phys docs related to case for the last — years

need to direct data custodians to preserve data

data retention policies are valid

ex: delete emails longer than 1 year

if this is in writing, then org is safe

but if they didnt follow policy then this data to be preserved

policy then
will need to be preserved

Video

surveillance used as defective control during investigation

ex'. attacker stealing data

Interviews

interview witnesses

Event Logs

recreate events before/during incident

what/when happened + account used

Sequence of Events

logs are primary source

. timestamps

Reports

develop report after analyze all evidence

document TTP used in attack

- findings & recs
- forensic tools used
- evidence
- findings from evidence
- recs based on findings

On-Premises versus Cloud Concerns

Cloud resources are add risk

org rarely knows exactly where data stored

Right to Audit Clauses

allows customer to hire auditors and review csp records

included in contracts

check security and controls

Regulatory Jurisdiction

where data is stored

must comply with location's laws

must comply

Data Breach Notification Laws

require orgs to notify customers about a data breach

depends on where stored

notification if org believes unauth entity acquired unencrypted PII

may be able to delay if law enforce says noti can impede investigation

include timeframe and possibly alert state attorney gen if high # of people affected

GDPR requires within 72 hours

Acquisition and Preservation

follow procedures to ensure data is not modified for forensics

Order of Volatility

order in which you should collect evidence

most volatile → least

Data in RAM is lost when pc is off

don't turn off suspect pc

order of volatility

- **Cache**
  removed as new data used
- **RAM**
- **Swap or pagefile**
  on system disk drive
  extension of RAM stored on hard drive
  rebuilt on reboot
- **Disk**
- **Attached**
  USB drives...

- Network
  servers / shared folders
  typically have robust backups

Data acquisition

snapshots - capture data for forensic analysis

artifacts - pieces of data on device that reg users are unaware of but forensics can extract

- web history
- recycle bin
- Windows error reporting
- remote desktop protocol RDP cache
  good for when attacker move laterally

OS forensics - collect data from OS like cache, RAM, swap file, artifacts

firmware forensics - extract firmware code and reverse engineer to id exploits

Forensic Tools

acquire, preserve, and analyze evidence

ensure data not changed while analyzing

Capturing Data

forensic image - collect data about mod

after saving image, create copy and analyze copy

dd - command to create images "data duplicator"

Kali linux has volatility framework - capture and extract mem contents digital artifacts

capture
and digital artifacts

memdump - dump any addressable mem space to terminal or redirect to file

WinHex - hex editor used for evidence gather, data anal, edit, recovery

FTK imager - forensic toolkit FTK capture image of disk as single/multi files

can do of individual files as well

Autopsy - GUI digiforensics

Verifying Integrity

Hashes and checksums

use to verify forensic images

provenance - tracing something back to origin

to origin

MD5 not used in crypto but still used in forensics

Bandwidth Monitors

network traffic capture tools can be used as bandwidth monitors

keep packet captures to help determine point of attack

Electronic Discovery

eDiscovery - id and collection of electronically stored info

vital to preserve metadata related to all files

metadata

- File

  when/who created

  mod/accessed dates

- Email
  header, who sent, when

- Web
  header, title, char set

- Mobile
  user location, phone calls, messages, web history...

Data Recovery

restoring lost data

from backups or even deleted data

can unformat drive

Strategic Intelligence and Counterintelligence

digital forensics intel - knowledge/info valuable to investigation from forensics

Strategic intelligence - collecting, processing to create long

Strategic intelligence - analyzing info to create long term plans/goals

digital forensics strategic intel - collect, process, anal digital data for long term sec goals

observe TTPs of attackers

counterintelligence - prevent or thwart spying

Protecting Data

data policies - assist in protection of data and help prevent data leakage

Classifying Data Types

help understand value of data

U.S. gov

U.S. gov

- Top secret
  could cause grave damage
- secret
  could cause serious damage
- Confidential
  could cause damage

sensitive data - any data not made public

Private companies

- Public data
- Private data
  info about person
  PII / PHI
- Confidential data
  info that org keeps w/ only certain groups of people

- **proprietary data**
  owned by individual, group, org
  patents, trade secrets, algos, designs...
- **financial information**
  any data related to money transactions
- **employee data**
  all orgs collected employee data
  name, addr, birth day, performance, payroll
- **customer data**
  info collected about customers
  email, username, pword, credit card, phone, addr

PII and Health Information

id someone

typically need 2+ pieces of info for it to be PII

company is liable for compromise of PII

Impact Assessment

helps org understand value of data by consider impact if lost/stolen

Data Governance

processes org use to manage, process, protect data

attempt to store data consistently

Laws and Regulations

- Health insurance Portability and accountability act HIPAA

orgs protect health info

1. health

orgs protect health
health of individual, health
plans for emp, ...

- Gramm-Leach Bliley Act GLBA
requires financial institutions
to provide consumers w/
notice explaining info
they collect and how used

- Sarbanes-Oxley Act SOX
requires executives to take
individual responsibility
for acc of financial reports
specs for auditing

- General Data Protection Regulation
GDPR
mandates protection of
privacy data for individuals
who live in EU
... what

who [illegible]

privacy notices - explains what info is being collected, how it's being collected, what used for, why, how used

critical data - data critical to success of mission

Privacy Enhancing Technologies

data minimization - requiring orgs to limit info they collect or use

Data Masking

modify data to hide og content

Anonymization

modifies data to protect privacy by removing PII

goal is to be permanent

[illegible] sometimes can undo

yes

but sometimes can undo

Pseudo Anonymization

replaces PII and other data with pseudonyms or artificial id

ex: name = Z1

separate data set is "key"

used when org wants to undo anon

Tokenization

replaces secure data w/ token - sub value

token system can convert token back to og value

Data Retention Policies

id how long data is retained and sometimes where stored

Data Sanitization

ensure data is removed or destroyed before disposing

ensure data is
from devices before disposing

Hard drives pose greatest risk

Common methods

- File shredding - overwrite space w/ I/O
- Wiping - writes diff patterns of I/O to ensure unreadable
- Erasing and overwriting
  SSDs use flash memory
  may just need to destroy
- paper shredding
- burning
- pulping
  reduces shreds to mash
- Pulverizing
  physically destroying media
- Degaussing
  powerful magnet

very powerful magnet
renders tape or disk unreadable

- third party solutions

UPS can shred

Training Users

train personnel on sec policies and keep up to date w/ tech and threats

Computer-based Training

training through app

Phishing campaigns

inform users of current phishing campaigns

Phishing Simulations

send fake phishing to employees

Gamification

assessments into user

Gamification

game design elements into user training methods

Capture the Flag

CTF - several challenges for players to solve

based on real-world cases

Role-based Awareness Training

target personnel based on role

Roles

- data owner
  - ensure data class correctly, labeled
  - adequate controls
- data controller
  - why/how personal data is processed
  - may be same as owner

may be ...

- **data processor**
  uses/manip data on behalf of data controller
- **data custodian/steward**
  routine tasks like back up, storage of data, implement business rules

  ex: db admin
- **data protection officer**
  id in GDPR

  ensure org comply with laws

Assessment notes

1. AUP - understand rules of behavior when access org sys
2. Mandatory vacations prevent emp from colluding

copy from cache)

3. least privilege = only enough perms as needed

4. Job rotation = switch roles

5. Preparation = take steps to prevent damage in future

6. Lessons learned = analyze previous incidents

7. Confiscation of physical asset didnt mention that it is a disk drive...

maintain chain of custody

8. Didnt see logs for given timestamp = didnt check time offset

offset

9. RAM and cache most volatile and need before turn off

you can take image of disk after power off

10. Forensic Analyst given drives to analyze

"assume" that chain of custody is already done

so creating hashes is correct

11. Masking = hide PII

anonymization same

tokenization does not protect

id

12. Anonymization = remove PII

13. Gamification to increase user engagement w/ learning

14. Data owners = classify and label data; make sure controls in place

15. Data protection officer = GDPR position for compliance and educate proper care of customer info