Chapter 8

Monday, August 21, 2023 2:03 PM

Understanding Risk Management

risk - likelihood that threat will exploit a vulnerability

Threats

threat - potential danger

any event or circumstance that compromise CIA

malicious human threats

accidental human threats

environmental threats

power, chems, natural disaster

threat assessment - helps org identify and categorize threats

identify/predict threats and find likelihood threat will occur

... life controls to protect against

identify controls to protect against

Risk Types

Risk types or categories

- Internal
  employees, hardware, software
- external
  external attackers
  natural threats
- IP theft
  copyrights, patents, trademarks
- Software compliance/licensing
  pirating licenses to software
  not properly managing who uses org's purchased licenses
- legacy systems and legacy platforms
  vendor stops supporting = no more patches for vulns

- multiparty
  if 3rd party partner is attacked
  it could expose org

Vulnerabilities

Vulnerability - flaw or weakness in software, hardware, or process that threat could exploit

default config
lack of malware protection or updated definitions
improper/weak patch management
lack of firewalls
lack of organizational policies

Risk Management Strategies

risk management - identifying, monitor, limit risks to manageable level

risk awareness - acknowledge risks exist and must be addressed

... that exists before

and must

inherit risk - risk that exists before controls are in place to manage

residual risk - amount of risk remaining after managing or mitigating risk

control risk - risk that exists if current controls do not adequately manage risk

risk apetite - amount of risk org willing to accept

Risk management strategies

- **Avoidance**
  not providing service or not participating in risky activity

- **Mitigation**
  implement controls to reduce risks

- **Acceptance**
  when cost of control outweighs a risk, accept the risk

- **transference**
  transfer risk to other entity or share
  insurance, 3rd party, ...

- **cybersecurity insurance**
  protect org/individuals from losses related to cyber incident

Risk Assessment types

risk assessment/analysis - quantifies or qualifies risks based on diff values or judgements

- first identify assets and values
- then identify threats and vulnerabilities and likelihood
- finally recs on what controls to implement

to implement

risk control assessment - examines org's known risks and controls in-place for them

risk control self-assessment - performed by employees

Quantitative Risk Assessment

measures risk using monetary amount

revenue value or replacement value

Model to determine risks

- single loss expectancy SLE - cost of any single loss
- annual rate of occurrence ARO - how many times loss will occur in a year

if <1, use a %

ex: once every other year

ex: once every
is 50%

- annual loss expectancy ALE - SLE x ARO

if cost of control is less than savings, buy it

if cost is greater than savings, don't

Qualitative Risk Assessment

uses judgement to categorize risks based on likelihood of occurrence and impact

impact - magnitude of harm from risk

may use surveys/focus groups

ex: experts rate probability and impact of risks of web server and library workstation

low, med, high

1 5 10

probability x impact

ex: 10 x 10

Documenting the Assessment

report showing risks and their suggested controls

very important to protect the report

Risk Analysis

identifies potential issues that could neg impact org's goals/obj

risk register - lists all known risks for system or org

living document

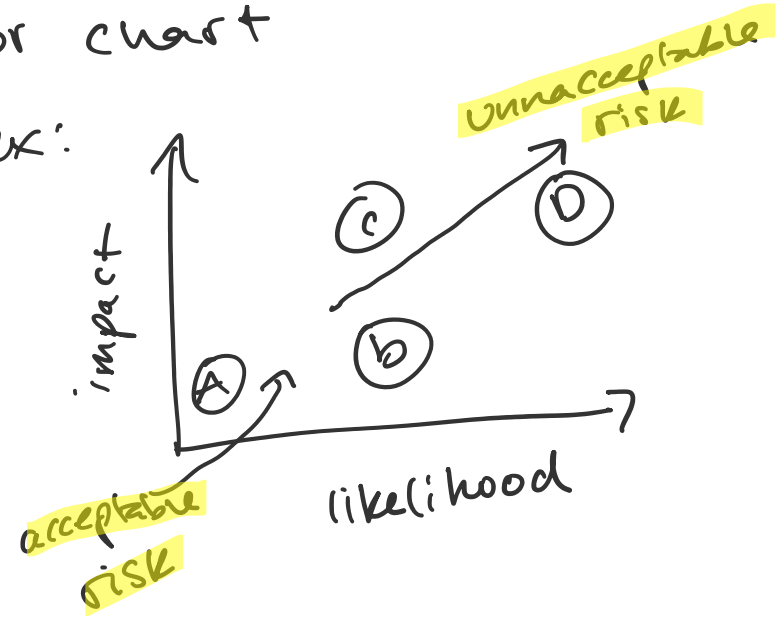
risk owner - responsible for implement security controls

- mitigation measures

- mitigation measures
- impact
- likelihood
- risk score

risk matrix - plots risks onto graph or chart

ex:



heat map - use colors rather than words

Supply Chain Risks

Supply chain - all elements required to produce and sell a product

mitigate risk by having multiple sources for everything it needs

Threat Hunting

actively looking for threats within a network before auto tool detects and reports

gather threat intel

- capabilities
- motives
- goals
- resources

threat feeds - sub to see up to date info on current threats

adversary TTP - attackers methods when exploit target

intelligence fusion - combine intel to create picture of likely threats and risks for org

Comparing Scanning and Testing Tools

vulnerability scanners - check for ...eaknesses + to exploit

vulnerability scanners - identify weaknesses

penetration tests - attempt to exploit vulns

Check for Vulnerabilities

Vuln assessments, scans (net & vuln)

Vuln assessment - assesses security posture of systems & networks

- review policies & logs
- interview emp
- test systems

High level steps of vulnerability assessment

- identify assets and capabilities
- prio assets by value
- identify vulns and prio them
- recommend controls

Password Crackers

attempt to discover pword

attempt to discover pword

usually hashed but w/ weak methods attacker can find pword or another pword w/ same hash

ex: MD5 = weak

offline - find pword by analyzing db or file containing pwords

ex: from data breach

online - guessing through brute force

log in remotely or collect net traffic

Network Scanners

network scanned - gather info about hosts in network

tool

hosts in

nmap - popular network scanning tool

- arp ping scan - any host that receives ARP packet responds w/ its MAC
- SYN stealth scan - sends SYN packet to each IP in scan range
  doesn't send ACK packet, sends RST (reset) packet
- port scan - checks for open ports on a system
  ex: port 443 open
- OS detection - analyze packets from IP to id the OS

TCP/IP fingerprinting

ex: TCP window size (size of receive window in first packet of TCP session) is not fixed

Linux ≃ 5,840 bytes

cisco router ≃ 4128 bytes

Cisco router ≃ 4128 bytes

Vulnerability Scanning

which systems are vulv to attack

- id vulns
- id misconfigs
- passively tests controls
- id lack of controls

Identifying Vulnerabilities and Misconfigurations

vuln scanners use db or dict of known vulns

ex: CVE

Common vulnerability Scoring system CVSS

assesses vulns and asigns severity score 0-10

Security Content Automation Protocol SCAP

uses national vulnerability database NVD - common misconfigs, software flaws, ratings/scores

flaws, ratings / scores

also use CVE and CVSS

Vulns related to weak configs

- **open ports and services**
  ex: web servers might not need TCP ports 20/21
- **unsecure root accounts**
  need strong pwords
- **default accounts and passwords**
  OS and apps have default accounts need to remove
  ex: SQL db allow sa (sys admin) account enabled w/ blank pword
- **default settings**
  use baseline to config
- **unpatched systems**
  scanners can detect lack of

scanners can detect the up-to-date patches or autoupdates

many patch management systems do this but vuln scan add extra layer

- **Cross**
  can compare against config or sec baseline to id common errors
- **Open permissions**
  common to secure files w/ permissions to prevent unauth access
  ex: leaving AWS buckets open to all
- **Unsecure protocols**
  ex: telnet
- **weak encryption**
  ex: SSL and not TLS
- **weak passwords**
  [illegible] scanners include password

- weak passwords
  many scanners include password crackers
- sensitive data
  scanners can have DLP to look for PII

can scan specific systems or entire network

Analyzing Vulnerability Scan Outputs

output typically has

- list of found hosts
- list of apps running on hosts
- open ports and services on hosts
- vulns
- recs to resolve vulns

Passively Testing Security Controls

vuln scans dont exploit vulns

passive

passive

pen tests are active

False positives and False Negatives

may report vuln that doesnt exist

ex: server doesnt have patches for db app but doesnt have db app

false neg

ex: patches applied to app server and breaks app

management accept risk of not applying patches

vuln scanner wont report

Credentialed versus Non-credentialed

credentialed vulnerability scan - use accounts credentials

without creds

accounts credentials

non-credentialed - without creds

cred scans usually use admin creds

- list software versions of apps
- lower impact on tested systems
- fewer false positives

attackers start as non-cred then use privilege escalation to do cred-scan

Configuration Review

configuration compliance scanner - performs config review

often use file as baseline

Penetration Testing

actively assess deployed controls in system or network

help determine impact of threat

extent of damage

extent of damage

also can run test to see how org will respond

view policies in action

pen tests can actually impact/disrupt operations

usualy use test servers/systems

Rules of Engagement

authorization before vuln/pen testing

boundaries of test

Reconnaissance

footprinting

learn as much as possibe about net

Passive and Active Reconnaissance

passive - collects info through OSINT

can also include collecting pub info about wireless net like SSID

info

SSID

the Harvester - gather public info like email, employee names, IP, URL

does not send info to get response from target but can send to other sources like whois.com or DNS servers

active - use tools/methods to engage target

Network Reconnaissance and Discovery

use tools to send data to systems and analyze responses

network + vulnerability scanners

- IP
- ports/services
- OS

Tools used in Recon

- **IP scanner**

  ping scanner

  searches for active IP

  Sends ICMP to range of IP in network

- **Nmap**

  cli network scanner

  - id all active hosts
  - host IP
  - protocols on hosts
  - OS of hosts

- **netcat**

  cli tool for admin to connect to Linux remotely

  banner grabbing - gain info about remote systems

  id host OS; can transfer files

- **Scanless**

  python based cli to perform port scans

scans

uses website so scans don't come from tester's IP

- **Dnsenum**
  enumerate DNS records for domains
  lists DNS records and id mail servers
  attempts to do AXFR transfer to download all DNS records but usually blocked

- **nessus**
  vulu scanner
  often for config reviews

- **hping**
  send pings using TCP, UDP, ICMP
  scan for open ports on remote sys

- **Sniper**
  auto scanner for vulu assessments
  ...ite edition

community edition

does scans

pro edition

can exploit

- curl

client URL

transfer and retrieve data to and from servers

ex: id all URLs of site and use curl to get all pages

Footprinting versus Fingerprinting

network footprinting - big-picture of network

IP addresses

fingerprinting - hones in on individual systems to provide details of each

[illegible] OS

systems

OS fingerprinting to find OS

fingerprinting is active

Initial Exploitation

after gaining info on vulns, then try to exploit

Persistence

attackers ability to maintain presence in a net w/out being detected

create backdoors

- make alt accounts
- enable SSH and create method to log on through SSH

Lateral Movement

exploit user pc and gain creds of user

use creds to access targeted system and uses for lateral movement -

use creds to [illegible]
and uses for lateral movement -
way attackers maneuver through net

ex: Windows management instrumentation
WMI and Powershell used to
scan Windows net

discover other systems, look for vulns
and exploits

Privilege Escalation

start pen tests by gaining access to
low-level user

tools like one click lets them in to
install RATs

then scan net to find vulnerabilities
to gain more privileges

Pivoting

process of using various tools to gain
more info

look for access to db, email, servers...

use exploited sys to target other sys

use exploited sys

known, Unknown, and Partialy known Testing Environments

Unknown environment testing - zero knowledge of env prios to test

black box

use fuzzing

known environment testing - full knowledge of env

white box

docs, code, login info

partialy known environment testing - some knowledge

gray box

maybe some docs info

Cleanup

remove all traces of pen-testers activity

remove all [illegible]

activities could include

- remove user accounts
- remove scripts/apps
- remove files
- reconfigure all settings

testers create log to remember

Bug Bounty Programs

monetary incentive for finding bugs

Intrusive versus Non-intrusive testing

intrusive - disrupt sys

non-intrusive - not compromise sys

pen testing = intrusive

vuln scanning = non intrusive

Exercise Types

test cyber readiness through competitions or training events

red team - attackers

- [illegible]

red team - attacker

blue team - defenders

purple team - both

white team - establish rules of engagement and oversee testing

Capturing Network Traffic

Packet Capture and Replay

packet capture - capture net packets over net

packet replay - send packets back out over net

use a network protocol analyzer

modify packet headers and payload

attackers can view unencrypted traffic by connecting unauth switch to capture traffic and forward to system using packet sniffer

server message block SMB - protocol to [illegible] over net

server message

send files over net

packet includes content of file

attackers can manipulate flags in packet headers for diff attacks

Ethernet II pane in wireshark

shows MAC addresses of source/dest

when using packet sniffer, enable promiscuous mode on NIC

Tcpreplay and tcpdump

Tcpreplay - suite to edit packet captures then send over net

used for testing

ex: modify packets to mimic attack and send to IDS

tcpdump - cli protocol analyzer

common to use tcpdump to capture and wireshark to analyze

Netflow, sFlow, IPFIX

Netflow - feature available on many routers that collect IP traffic and send to netflow collector

does not show payload data or even headers

only shows counts/stats

What to expect in Netflow packets

- timestamp for start/finish of flow
- input interface id (router/switch)
- output interface id (0 in packet dropped)
- source/dest info
- packet/byte count
- protocol

sFlow - sampling protocol

traffic info based on preconfiged sample rate

ex: 1 out of every 10 packets

good for high volume

IP Flow information export IPFIX

very similar to Netflow v9

alt/replacement to Netflow

Understanding Frameworks and Standards

framework - structure to provide a foundation

key Frameworks

International organization for Standardization ISO - independent org that establishes standards

ISO 27001 - "information security management"

info sec management system ISMS

reqs

certification

ISO 27002 - "info tech sec techniques"

compliment to 27001

best practices

ISO 27701 - "Privacy info management system" PIMS

based on 27001 and use for manage and protect PII

guidance for compliance

ISO 31000 - family of standards related to risk management

Auditing standards board of the american institute of certified public accountants AICPA

published audit standards

Statement of standards for attestation engagements SSAE

guidance on creating reports

System and organization controls SOC 2

organizational security controls

System [illegible]

organizational security [illegible]

created after auditing controls

addresses CIA + sec + privacy

SOC 2 type 1 - describes org's systems and describes design effectiveness

how well controls address risks

on a specific date

SOC 2 type 2 - systems and controls

effectiveness over range of dates

how well they mitigated risks

Center for internet security CIS - provide

best practices and maintain info

on threats

Risk Management Framework

-- risk manage framework

Risk manag.

NIST SP 800-37 Risk manage framework
for info systems and orgs

US fedr have to adopt

NIST RMF

- Prepare
  - id key rdes to implement frame
  - risk tolerance strats
  - Update/create risk assess
  - id in-place controls
  - continuous monitor strat
- categorize information systems
  - determine impact to ops if loss
    - in CIA
  - prio systems
- select security controls
  - typically start w/ baselines

- typically start w/ baselines
- implement security controls
- Assess security controls
- Authorize information systems
  senior management decides if system is gtg
- monitor security controls
  constantly assess changes in sys and env

risk assessments

NIST CSF aligns w/ RMF

NIST CSF components

- Framework core
  set of activities that org can select to achieve outcomes

1. Identify
2. Protect

2. Protect
3. Detect
4. Respond
5. Recover

- Framework Implementation tiers
  id how org views risk
  1. Partial
  2. Risk informed
  3. Repeatable
  4. Adaptive

  Adaptive is highest and means it needs mature risk manag program

- Framework Profiles
  list of outcomes for org based on its needs and risk assess

current & target profiles

Reference Architecture

a doc or set of docs that provide set of standards

Exploitation Frameworks

tool used to store info about vulns

- metasploit framework
  - open linux
  - over 1600 exploits
- BeEF browser exploitation framework
  - web browsers exploit frame
- W3af web app attack and audit framework
  - web app vulns

Benchmarks and configuration guides

Benchmarks and configuration

Windows / Linux guides to id secure settings

follow guides for specific system you're setting up

Assessment Notes

1. ALE = SLE x ARO
2. Risk register = doc with known risks + risk scores
3. Supply chain assessment = find all elements to support this site
4. Threat hunting is actively looking for threats before auto tool detects them

- intelligence fusion
- vulnerabilities and bulletins

- advisories and bulletins
- threat feeds
- preds on how attackers may maneuver in net

5. Nmap is a network scanner can detect protocols and services running on server

6. Port scanner finds open ports and can then id services running on system

protocol analyzer would be much harder to do this

7. False - = scan returns nothing even if you know its missing patch

8. Vulnerability scan best to verify has or to date patches

8. Vulnerability scan = system has up to date patches

9. Credentialed scans reduces false +

10. Lateral movement or pivoting is attempt to access other systems after gain access of I

11. Need rules of engagement before running pen tests or vuln scans

12. Outsourced to modify existing app. Even if testing with full app, this is still partially known env

13. Red team = perform simulated attacks

14. PCI DSS = payment cards info

15. TCPreplay is best to verify IDS will detect syn stealth attack

will detect syn stealth a.

can use to capture/modify packets

to simulate attack

need to send packets in this

scenario