Introduction

04 August 2020 18:34

- Identify threat
- Respond to event
- Investigate effects of threat further

CIA Triad

Confidentiality — Data remains private to those with proper access

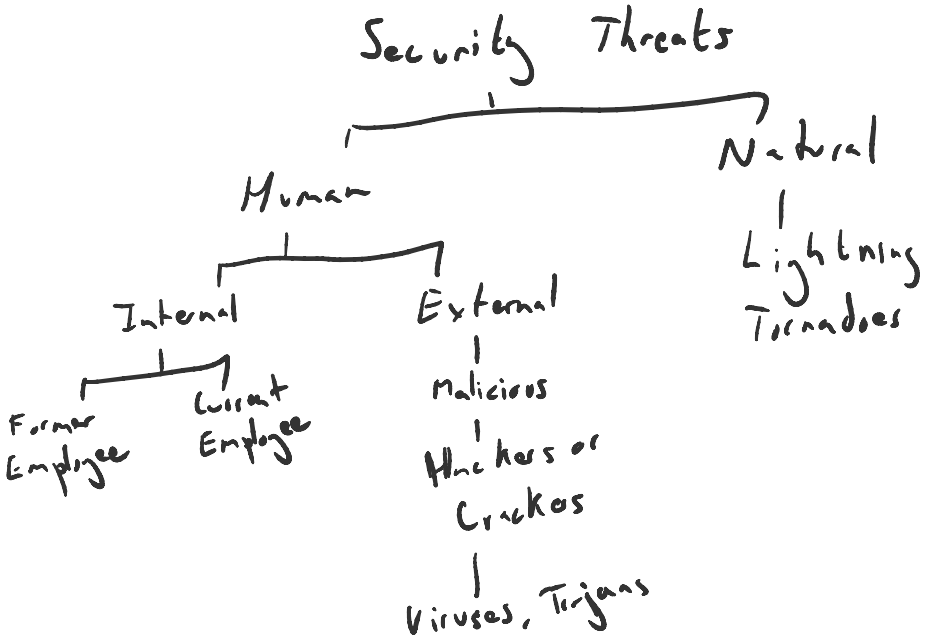
Integrity — Data remains accurate - can check hash values of data and downloaded data

Availability — Routine maintenance, upgrading software and hardware

KEY TERMS

Vulnerability	Flaw, loophole, oversight, error that can be exploited
Threat	Event: natural or man-made that can cause negative impact
Exploit	A way to breach a system through a vulnerability
Risk	Probability of event happening

SECURITY THREATS



VULNERABILITY ASSESSMENT

Search for weaknesses in order to apply a patch or a fix to prevent compromise

How do they occur?
- Products shipped with known or unknown bugs and faults
- Vulnerabilities as a result of misconfiguration by user/administrator

ROLES

Common roles:
CISO (chief information security officer) - high level, supervisor of security of entire department / company
Information Security Architect
IS Consultant
IS Analyst - analyse events, alerts, alarms and collect information that could be used to identify threats
IS Auditor - testing effectiveness of computer systems and reporting (ISO 27001/2?)
Security Software Developer
Penetration Tester/ Ethical Hacker aka part of Red Team
Vulnerability Assessor (blue team)

Early military operations:
Clipper chip - installing spy chips in phones
Moonlight Maze - dumping of linux system passwords (Russians did this attack using tool called lucky tool)
Solar Sunrise - series of attacks on department of defense computer network. Creating a backdoor
Buckshoot Yankee - significant, USB drive insertion, trojan horse, 14 months
Desert Storm and Bosnian wars - radars tampered with fake information

Setup a Cybersecurity Program

Identify threats and risk
Create teams

Procedures, standards, user education
Incident response, disaster recovery, physical security

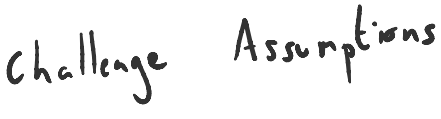
Classification, implementation, assets
Documentation

Network infrastructure, endpoints, servers, id management
Vulnerability management, monitoring, logging

Additional Security Challenges

Simple requirement can have many complex solutions
Security architectural decisions
Key management
Protectors have to be right all the time - attackers just once
No one likes security until its needed - often an afterthought and not baked in

CRITICAL THINKING



Question your way of thinking
Gather more data

Our brain can piece something together with very little data
Failure to consider missing data can be dangerous

J

Question your way of thinking
Gather more data
Take a systematic and logical approach
Assess each assumption

Explanations

Our brain can piece something together with very little data
Failure to consider missing data can be dangerous
Brainstorm, consider who/what/when etc.
Null hypothesis

Evaluate Data

Establish a baseline of what normal is
Establish anomaly detection, what's inconsistent?
Assess against multiple hypotheses to see goodness of fit
(Scientific method)

Identify Key Drivers

Significantly impact a situation
Technology, regulation, society, supply chain, employees, threat actors

Understand Context

Understand operation environment
Consider perspective of others
Problem Framing - if a problem can't be solved in it's given frame then try reframing
I.e. Slow elevator problem = waiting is boring problem