Understanding Risk Assessment

Risk The likelihood that a thread will exploit a vulnerability

- A **vulnerability** is a weakness, and a threat is potential danger
    - If your anti-virus software is not up to date- that is a threat malware can reach your network

The likelihood of a risk occurring is not 100% - An isolated system without internet access has a low chance of a malware infection.

- You can’t eliminate risk; you can just mitigate it

Threats and Threat Assessments

A threat is potential danger. Within the context of Risk Management.

- A threat is any circumstance or event that can compromise confidentiality, integrity or availability of data on a system

Malicious human threats.

- Threat actors include inexperienced script kiddies, dedicated criminals working within an organized crime group, and sophisticated advanced persistent threats (APTs) sponsored by a government

Accidental Human Threats- Users can accidently delete or corrupt data or accidently access data they should not be seing. Even systema admins can accidently take down a system. For example in the attempt to fix one problem, a system admin can take down the system by accident
Environmental Threats- This includes long tern power failure, chemical spills, pollution, or natural threats such as hurricanes, tornados, earthquakes etc….

Threat Assessments

A threat assessment helps an organization identify and categorize threats. It attempts to predict threats against an organizations assests along with th elikelyhood a threat will occur.

The assessment also attempts to identify the potential impact from these threats.

Organizations have limited resources so it’s not possible to protect against all threats.

Common types of Assessments

Environmental- An environmental threat assessment evaluates the likelihood of an environmental threat happening. For example if you live in Virginia and a hurricane hits every 3 years. The likelihood of your company suffering hurricane damage is 33%
The likelihood of living in Virginia and your company suffering damamge from an earthquake is about 1%.

Manmade- This is threat from humans. This refers to an attack from any person or groups of people. There are also accidental human ocuurances.

Internal- This is a threat from within the organization. This includes threats from malicious employees and also hardware falure.

External- This is a threat assessment from outside the organization.

Vulnerabilities

A vulnerability is a flaw or weakness in software or hardware that can result in a security breach. Lack of updates – If systems aren't kept up to date with patches and hotfixes, theyare vulnerable to attack.

Default configurations- Hardening a system includes changing systems from their default configurations including changing default usernames and passwords

Lack of malware protection or updated definitions- If malware protection is not kept up to date th esystems are susceptible.

Lack of Firewalls- If firewalls are not enabled or configured properly networks are vulnerable to attacks.

Lack or organizational policies- If job separation, mandatory vacations, and job rotation policies aren't implemented, an organization is suseptable to fraud and collusion from employees

Risk Managment

Risk management is the practice identifying, monitoring and limiting risks to a manageable level. The primary goal of risk management is to reduce risk to the level that an organization wil accept.

Multiple Risk Response Techniques include:

Avoid- An organization cann avoid a risk by not provide a service or not participating in a riskier activity. For example an orgab=nization may be considering purchasing a piece of software that rewuires multiple opn ports on a firewall. If its too much of a risk they may decide not to purchase the software.

Transfer- The organization transfers or shares the risk with another rentity. The most common example of this is purchasing insurance

Mitigate- The organization implements controls to reduce the risks. These controls either reduce the vulnerabilities or reduce th eimpact of the threat.

Accept- When th ecost of the control outweighs a risk, an organization will often accept the risk.

Risk Assessment

A risk assessment or risk analysis is an important task in risk management. A risk assessment starts with identifying assests and their value.

An asset includes any product, system, resource, or process that an organization values. It can be a specific monetary value or subjective value such as Low, Medium, and High. The asset value helps an organization focus on high value assets and avoid wasting time on low value assets.

A risk assessment is a point in time assessment or a snapshot in time.

Risk assessments use quantitive measurements or qualitative measurements.

Quantitative measurements use numbers, such as a monetary figure representing cost and asset values. Qualitative measurements use judgements.

Quantitative Risk Assessment

This tupe of measurement is using a monetary amount.
This monetary amount makes it easier to prioritize risks.

The assest value may include the revenue value or replacement value of an asset.

If web server fails , the company will lose $10000 in direct sales every hour it is down plus the cost to repoair it.

IN contrast the failure of a library workstation may cost a one time fee of $1000 to replace it.

Commonly Used Quantitative Models

SLE- Single loss expectancy- The SLE is the cost of any single loss.
ARO Annual Rate of Occurance The ARO indicates how many time the loss will occur in a year. If the ARO is less than 1, the ARO is represented by a percentage. If you anticipate something happening once every two years the ARO is 50% or .5
ALE Annual loss expectancy The ALE is the value of SLE x ARO

Quantitative Loss Examples

Employees lose the average of one laptop a month because they forget and leave their laptop in aconference room. There are thieves who steal these laptops fom the conference rooms.
It was suggested that locks be purchased at the cost of $1000 to protect these laptops
Is it worth it to purchase these locks
SLE Value of each laptop is $2000 so the SLE is $2000
ARO, One laptop is stolen each month so ALO = 12
ALE- You calculate the ALE as SLE x ARO so $2000 x 12 = $24000
Security experts estimate this will reduce the number of stolen laptops from 12 a year to 2.
The changes the ALE from $24000 a year to $4000 a year. This saves $20000 a year. In other words if the organization spends $1000 they will save $20000.

What happens if you don’t know the ARO

Use algebra
ALE = SLE x ARO
ARO = ALE/SLE
SLE = ALE/ARO

Qualitative Risk Assessment

A qualitative risk assessment uses judgement to categorize risks based on likelihood of occurrence of probablility and impact. The likelihood of occurrence is the probablility that an event will occur such as the likelihood that a threat will attempt to exploit a vulnerability. Impact is the magnitude of harm resulting from the risk
Notice this is much different from the exact numbers provided by quantitative assessment that uses monetary figures.
You can think of quantitative as using a quantity where qualitative is related to quality and is often a matte rof judgement.

Qualitative Risk Assessment

• Identify significant risk factors
• Ask opinions about the significance • Display visually with traffic light grid or similar method
Business impact analysis
• What are your critical business functions? • Define the important business objectives
What is impacted?
• Loss of revenue, legal requirements,
customer service
How long will you be impacted?
• You'll need personnel, equipment, resources
What's the impact to the bottom line?
• Is disaster recovery a good investment?
Testing for risk?

Qualitative Risk Assessment The Challenge

One of the challenges with qualitative risk assessment is gaining consensus on the probability and impact.
Unlike monetary values that you can validate with facts, probability and impact are often subject to debate.

Documenting The Assessment

The final phase of risk assessment is writing the report
This identifies the risks found and the recommended controls.
A simple example is a database enabled web application may be susceptible to SQL injection attacks. The risk assessment will then recommend rewriting the web application with input validation techniques or stored procedures to protect the database.

Points To Remember For Risk

It is not possible to eliminate Risk but it is possible to manage it. An organization can avoid a risk by not providing a service or not participating in a risky activity. Insurance transfers the risk to another entity. You can mitigate risk by implementing controls, but when the cost of the controls exceeds the cost of the risk, an organization accepts the remaining or residual risk.

Comparing Testing and Scanning Tools

Two common categories of tools:
Vulnerability scanners check for weakness
Penetration tests attempt to exploit the vulnerabilities discovered by the vulnerability scan or from some other means.

What’s included in a Vulnerability Assessment

The following high level sections are typically included in vulnerability assessments:
Identify assets and capabilities
Prioritize assets based on value
Identify vulnerabilities and prioritize them
Recommend controls to mitigate serious vulnerabilities

Common Tools Used In Vulnerability Scans and Assessments

Passsword Crackers
Network scanners- these use various techniques to gather information about hosts within a network
A. Ping Scans- see if a server responds
B. Arp ping scan – Any host that receives an ARP spacket with its IP address responds with a MAC address
C. Syn stealth scan – This is used in the three way handshake. A single SYN packet is sent to each IP address in the scan range Instead of responding with an ACK packet the scanner typically sends a RST reset response to close the connection
D. Port Scan – Checks open ports in the system
E. Service scan A service scan is like a port scan but goes one step further. A port scan identifies open ports and gives a hint as to what protocols may be being used. The service scan verifies the protocol or service. Lets say a port scan identidfies port 80 is open. A service scan will now send an HTTP commandsuch as “Get/.”if HTTP is running on port 80 will respond to the GET command thereby verifying that this is a web server.
OS Detection OS detection techniques analyze packets from an IP address to identify the OS Operating System

Network Mapping

Network mapping detects devices on a network and how they are connected to each other. Tools used to do this are NMAP used along with Zenmap that provides you with a graphical representation of a network

WARNING- Do not do this on a corporate or public network. You may face legal challenges if you run network scans on networks you do not own or control. Ideally you would run these to practice on a PRIVATE network in your home that you control. This means the packets do not leave your house. Scanning a netwok on virtual box on your computer would fit this scenario.

WiFi Scans

Wireless scanners can use passive or active scans
A passive scan just litens all the traffic being broadcast on a network
An active wireless scanner such as Acrylic WI-FI Profesional has many capibilities
See this link for details:
https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wifi-analyzer-acrylic-professional/

Rogue System Detection

An administrator would know all SSIDs (Local networks available to connect to)
Administrators can investigate any unknowd SSID’s

Lack of Security Controls

A vulnerablility scanner can identify vulnerabilities, misconfigured systems, and the lack of security controls such as up to date patches
Vulnerability scans are passive and have little impact on a system during a test. In contrast a penetration test is intrusive and can potentially compromise a system.

Penetration Testing

Because Penetration tests can disrupt operations, they are often performed on test systems which are a replication of the live environment.
Many penetration tests include the following activities:
Passive reconnaissance
Active reconnaissance
Initial exploitation
Escalation of Privilege
Pivot- once you gain acssess to someones computer you use that computer to spy on others in network
Persistance- techniques that allow testers to remain in a network for weeks such as creating accounts that can be accessed remotely

Exploitation Frameworks

This is a tool used to store information about a security vulnerability. It is often used to detect and exploit software
Metasploit Framework An open source framework that runs on Linux It has data on over 1600 exploits. Includes methods to exploit code
BeEF Browser Explotation Project Open source web brower project designed to exploit weaknesses in web browsers
W3af Web Application Attack and Audit Framework Open source framework focuses on application vulnerabilities

Other Commonly Used Tools

Wireshark GUI Tool
Command Line Tools –
TCPdump
NMAP
Netcat

Risk Registers

Some risk assessments use Risk Registers
A risk register is a repository for all the risks identified. Here is what one might look like
Category
Specifric Risk
Likelihood of Occurrence
Impact
Risk Score
Mitigation Steps
Contingencies
Risk Score with Security Controls
Action Assigned to
Action Deadline

Supply Chain Assessment

A supply chain includes all the elements required to produce and sell a product.
A supply chain assessment evaluates these elements- the raw materials supply sources and all the processes required to create, sell and distribute the product.
What is the risk? For example, if Tesla needs litium to make batteries for its cars what is the risk if the ssuply sources of Lithium become disrupted?

Points to Remember

A risk register is a comprehensive document, listing known information about risks.
It typically includes risk scores along with recommended security controls
A supply chain assessment evaluates everything needed to produce and sell a product.
It includes all the raw materials and processes required to create and distribute a finished product