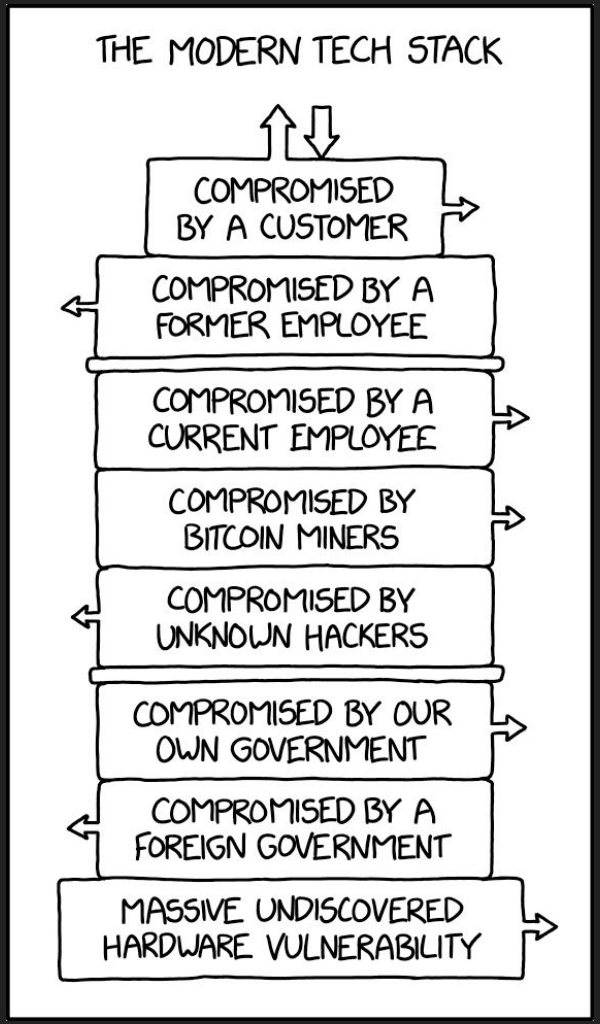
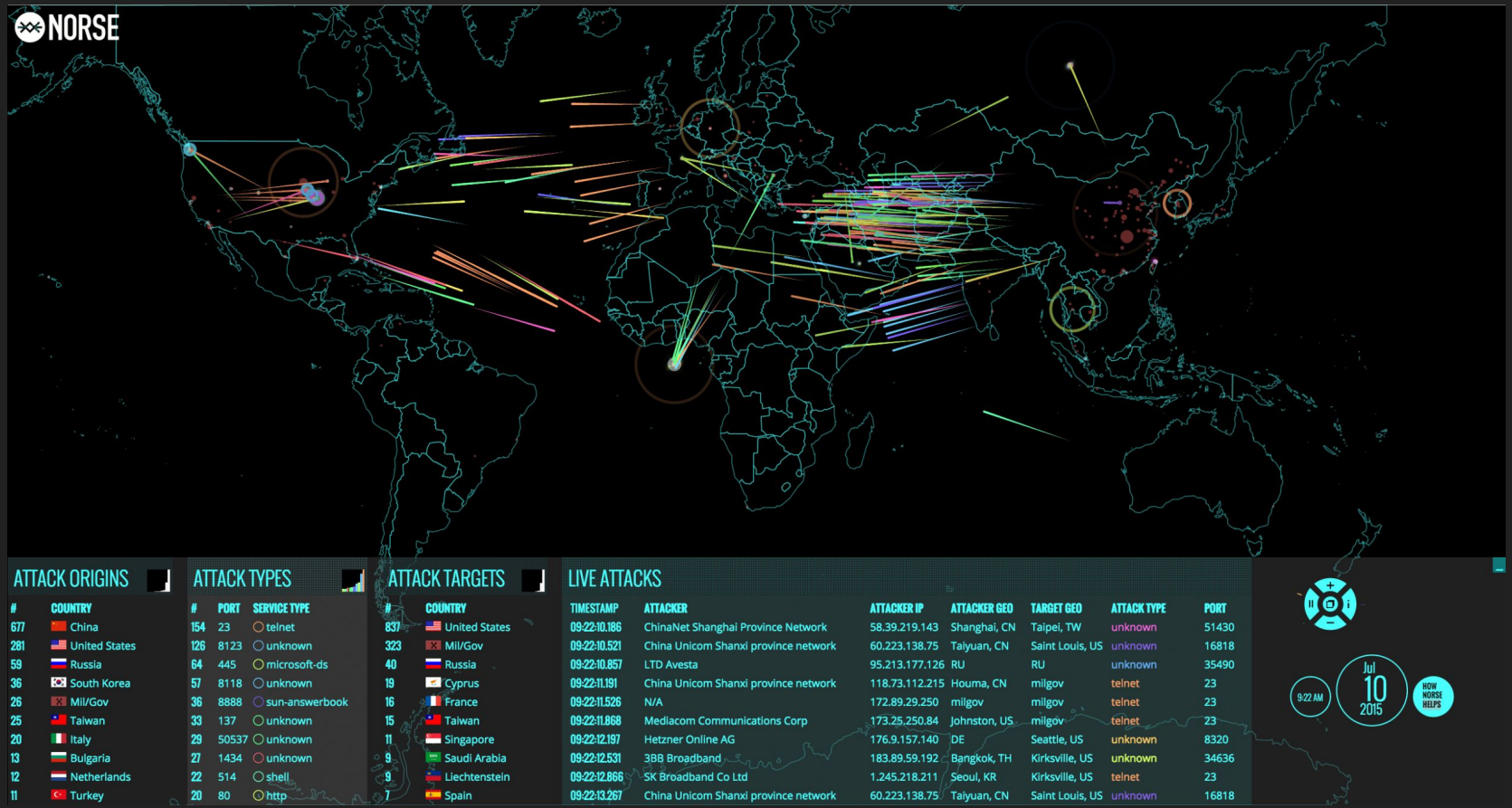
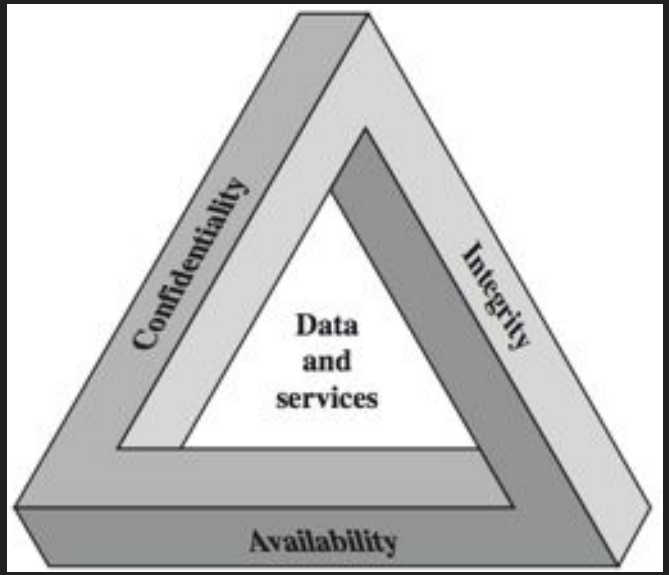
Digital Security


THE MODERN TECH STACK
COMPROMISED BY A CUSTOMER
COMPROMISED BY A FORMER EMPLOYEE
COMPROMISED BY A CURRENT EMPLOYEE
COMPROMISED BY BITCOIN MINERS
COMPROMISED BY UNKNOWN HACKERS
COMPROMISED BY OUR OWN GOVERNMENT
COMPROMISED BY A FOREIGN GOVERNMENT
MASSIVE UNDISCOVERED HARDWARE VULNERABILITY

Networks are targets



How do we define electronic security?



Computer/Network Security - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **confidentiality**, **integrity**, and **availability** of information system resources

Security Requirements

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

Guarding against information modifications or destruction, including ensuring information non-repudiation and authenticity

Availability

Ensuring timely and reliable access to and use of information

Network Security Basics

Protection

- Configure your systems and networks as correctly as possible with many layers of security (Defense in Depth)

Detection

- Must be able to identify when the configuration has changed or when some network traffic indicates a problem

Reaction

- After identifying problems, must be able to respond to them and return to a safe state as rapidly as possible

Types of Attacks

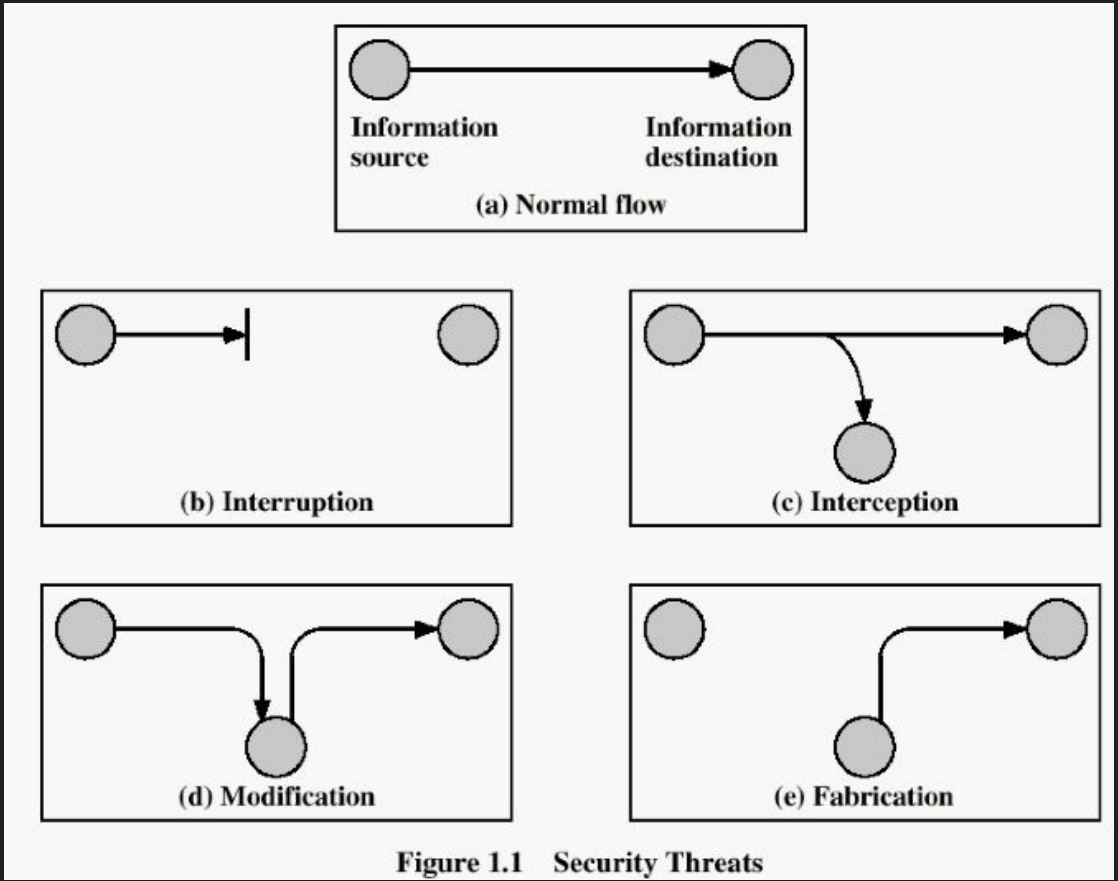


Figure 1.1 Security Threats

Common Security Threats

Denial of Service

Denial of Service (DoS)

- the goal of DoS attack is to degrade service to the point that legitimate users are unable to conduct their regular activities

Distributed Denial of Service

- A scaled up version of a DoS attack often using a botnet of infected computers thereby using several internet connections simultaneously to overwhelm the target

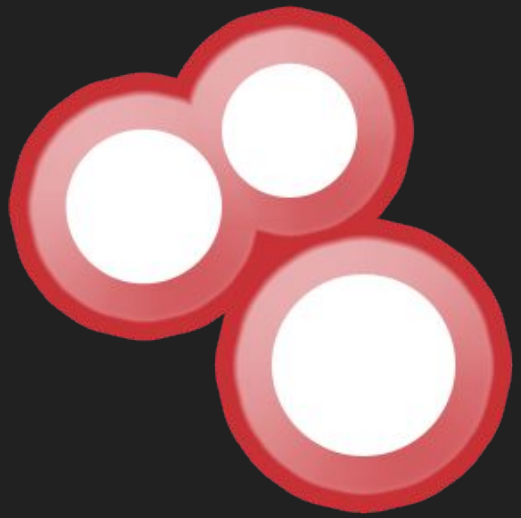
Scanning/Probing

Scanning/Probing usually precedes an attack to gain access by discovering information about system or network

The goal is to discover what services or systems are accessible as well as potential known vulnerabilities that can be exploited

Probe refers to an individual attempts, whereas a scan consists of a large number of probes by an automated tool

Scanning/Probing



SHODAN

Viruses & Worms

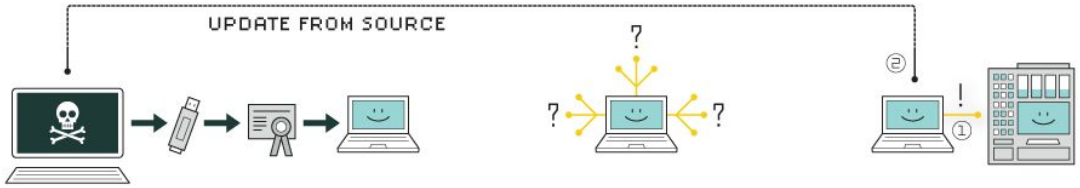
Both Worms and Viruses are cases of malicious code, usually with the goal of remaining hidden in the system until the damage is discovered

The difference between viruses and worms is the way they auto-replicate

- Worms propagate without any human intervention
- Viruses need some kind of action from a human (unknowingly downloading, installing, etc)

Viruses & Worms

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

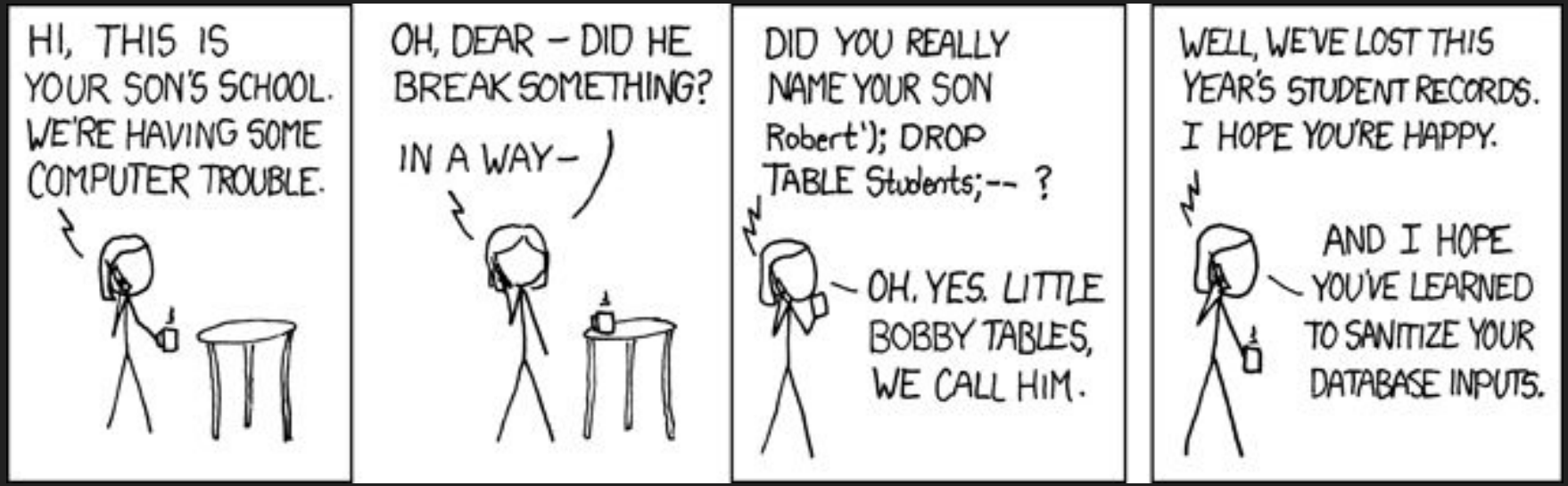
Viruses & Worms

Viruses & Worms

Injection Attacks

An injection of code happens when an attacker sends invalid data to the web application with the intention to make it do something different from what the application was designed/programmed to do

"SELECT * FROM accounts WHERE ID = '" + request.getParameter("id") + "'";



Broken Authentication

A broken authentication vulnerability can allow an attacker to use manual and/or automatic mediums to try to gain control over an account

- Weak Passwords are easily cracked
- Passwords that are never changed
- Shared users/credentials across services
- Plain-text passwords stored in the database
- No lockout policy to prevent brute-force attacks
- Bad session management which allows hijacking of privileged accounts
- No MFA support

Authentication vs Authorization

Authentication

the act of validating that users are who they claim to be

- Possessing or carrying the correct key or token
- Knowing predetermined private information
- Providing information that is inherent and unique to that individual

Authentication vs Authorization

Authorization

the process of giving the user permission to access a specific resource or function

- permission to access an application/resource
- providing administrative rights to a server

Authorization must always follow authentication

users should first prove that their identities are genuine before an being granted access to the requested resources.

Misconfiguration/Oversight

One of the most common ways attackers gain unauthorized entry is due to misconfiguration or oversight.

- Default Credentials!
- Systems exposed directly to the internet
- Running unnecessary services
- Running policies of Allow by Default
- Accidental mistyping (no audit in place to catch it)

- This can occur at every layer of the technology stack

Using components with Known Vulnerabilities

Failing to update every piece of software, library, operating system, etc...
without a doubt, introduces heavy security risks sooner rather than later

The question is, why aren’t we updating our software on time?
Why is this still such a huge problem today?

- Can’t keep up with the update schedule - too many updates to always be up to date
- Legacy Code - won’t work anymore with newer versions of its dependencies
- Technical Debt - running code in production that cannot be upgraded without downtime or required high effort due to previous architectural decisions

Insufficient Logging and Monitoring

While 100% security is not a realistic goal, there are ways to keep your systems monitored on a regular basis so you can take immediate action when something happens

Not having an efficient logging and monitoring process in place can increase the chances of system compromise as well as the amount of time an attacker has before detection

Leads to a false sense of security - no alerts, everything must be fine

- The inverse is also true - if everything is alerting all the time then important messages get lost or ignored

Social Engineering

Phishing

The practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information

Vishing

The practice of eliciting information or attempting to influence action via the telephone, may include such tools as “phone spoofing“

What defenses do we have?

Zero Trust Architecture

The Zero Trust Model treats every transaction, movement, or iteration of data as suspicious and inspects actions both within the network itself as well as at the boundaries

Method of Least Privilege - Have a default policy of deny all and only grant what is explicitly required for functionality

As with all forms of security, it is a tradeoff between convenience/usability and security

- The more security measures that are in place, the harder a system is to use

Zero Trust Architecture

Network Layout

Time to revisit network planning! The layout of your network greatly determines what controls can be put in place and the potential threat landscape

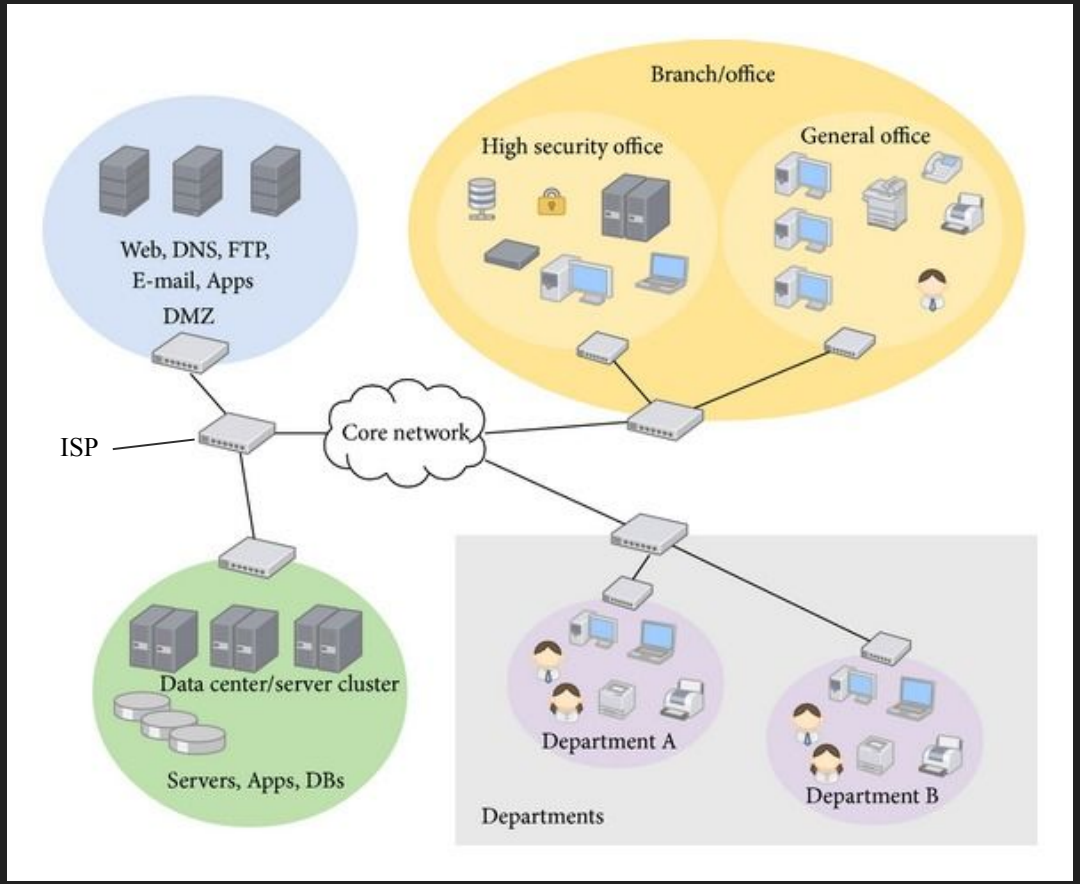
Network Segmentation - isolate systems that do not need to talk to each-other on seperate networks to reduce **lateral movement**

- Classify all traffic based on endpoint identity
- Implement access controls at each segment layer

Lateral Movement - a set of techniques attackers use to move around devices and networks and gain higher privileges

- Once attackers infiltrate a system, they map all devices and apps in an attempt to identify vulnerable components to infiltrate

Internal vs External Networking



Network Layout

Now that we have servers in the internal network, we need some way to allow external users to access them.

To accomplish this, we often use the following methods

- Put the external server in a External DMZ
- Use Port Address Translation (PAT)
- Use a Load-Balancer

To allow services on the internal network to get to the internet we need to use Network Address Translation (NAT) on the gateway.

Diagram out NAT, PAT, LB on the board

Firewalls

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet

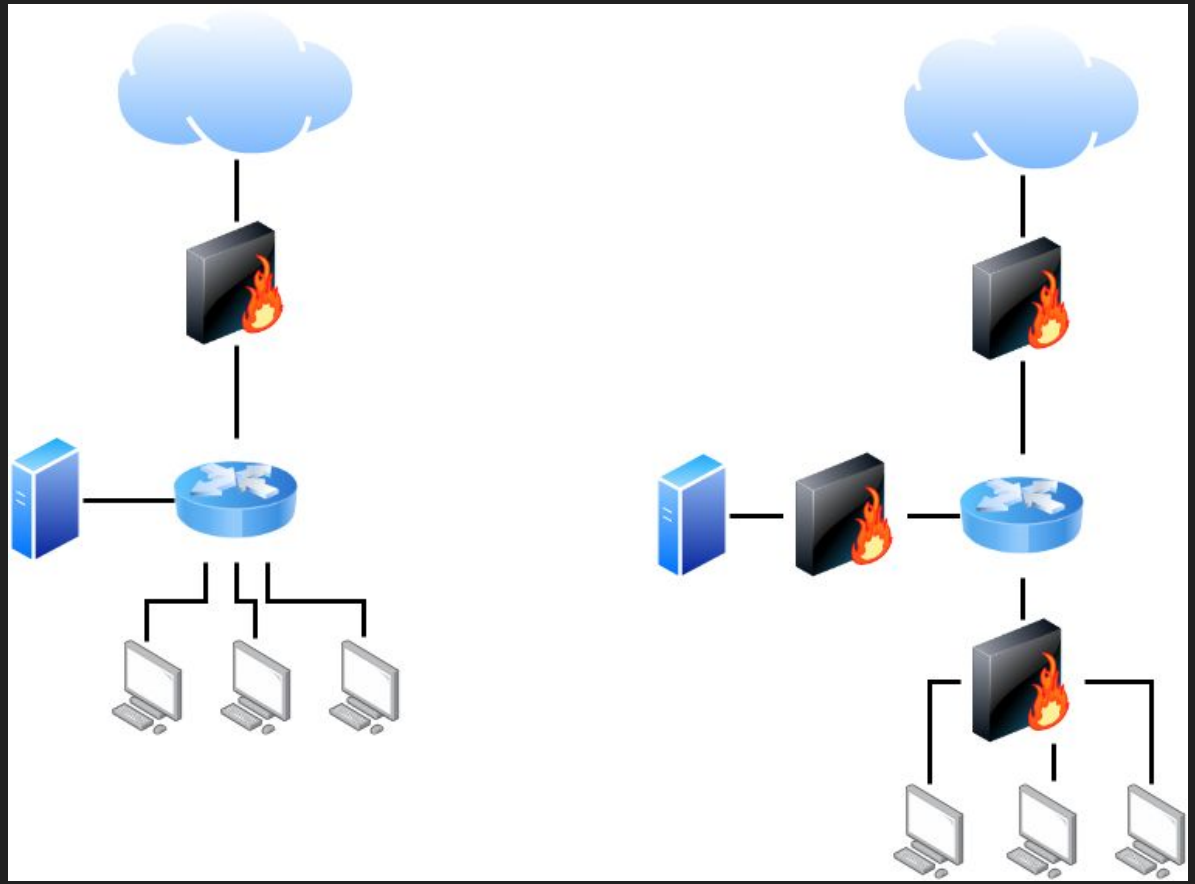
- Depending on your network layout there may be several layers of “Internal Networks” with firewalls between each

They use a set of defined rules to allow or block traffic

- Rules are comprised of a set of IP ranges or Subnets and actions to permit or deny
- Examples can be as broad or specific as
  - Subnet A can talk to Subnet B
  - Machine with IP X can talk only to Machine with IP Y on Port 22 using an established TCP connection

A firewall can be hardware, software, or both and can reside as a network appliance, or on an endpoint

Firewalls



Network Access Control (RADIUS)

Not every user should have access to your network

To keep out potential attackers, you need to recognize each user and each device

- Can determine if the machine is up to date, has required anti-virus installed, etc
- Can work with Authn/Authz systems to identify the user and what network access they should have

Then you can enforce your security policies

- You can block noncompliant endpoint devices or give them only limited access
- Policies can be enacted on a per machine or per user basis - allows for locking down network traffic based on authorization

Intrusion Prevention Systems

An intrusion prevention system (IPS) scans network traffic and attempts to actively block attacks.

It does this via:

- Detecting unwanted behavior
  - Signature-based detection - based on a dictionary of uniquely identifiable patterns in the code of each exploit determines when an exploit is traveling through the network
  - Statistical anomaly detection - often combined with machine learning to determine the ‘normal’ state of the network and can alert on deviating network traffic
- Taking action to prevent the unwanted behavior
  - Sending an alarm to the administrator (as would be seen in an IDS)
  - Dropping the malicious packets
  - Blocking traffic from the source address
  - Resetting the connection
  - Quarantining a potentially compromised server

VPN Tunnels

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet

Typically used to connect internal networks/services over the internet without exposing the services to the internet itself

- VPN configurations and credentials are high value targets for attackers
- Can be both another threat vector as well as helping to close off other threat vectors

Can also be used to mask traffic and make it seem like traffic is coming from somewhere else

- Unknown VPN use is a Red Flag and is often blocked by IPS as it can be used for data exfiltration

Anti-Virus/Anti-Malware

Good AV/AM should not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage

Not the silver bullet some places believe it to be, however not something to be discounted either

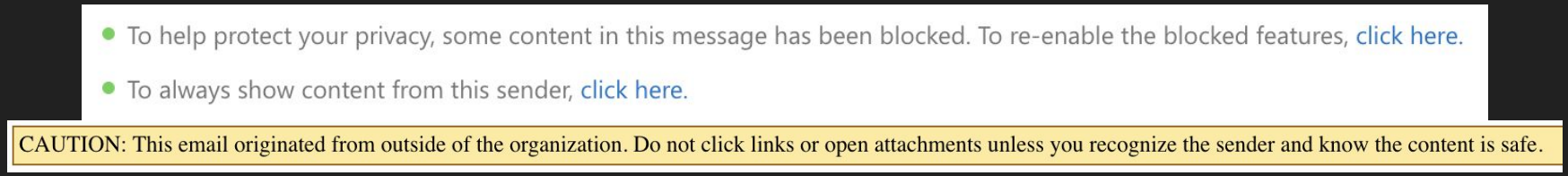
Email Security

Email gateways are the number one threat vector for a security breach

Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware

Anti-Spam and Anti-Malware filters

- Can be used at the Email Gateway level to detect phishing attempts and attached malware
  - Flag emails based upon ACLs, previous metrics and learning based on user feedback



- Policy Implementations
  - Prevent users from sending attachments (or attachments that are executable)

Web Security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites

Often implemented in the form of a Proxy Server

- Can handle blocking web requests based on whitelist/blacklist and also by content inspection
- Used in conjunction with network access controls to force configuration and allow/disallow internet access altogether

Can block egress traffic to unknown hosts and prevent exfiltration of data

- Often can be combined with a Data Loss Prevention (DLP) solution to check for traffic that includes PII, Corporate Secrets, etc and block or redact the traffic in flight

Wireless Security

Wireless traffic within data centers are another potential attack surface

If someone gets physical access they can deploy a device that communicates wirelessly (over WiFi, or 3G/4G)

To mitigate this, high security data centers are often built with thick exterior walls and use materials within the computer rooms to prevent wireless transmissions

For environments that require wireless networking, ensure proper encryption schemes are used - WPA2 / WPA2-Enterprise

What about the human element?

Training and Policy

Establishing good security policies and providing training for users are some of the best ways to increase defenses in the human element

- Social Engineering Training (Phishing/Vishing Examples)
- Determine which problems need to be solved by policy and which need to be solved or reinforced by technology
  - i.e. A policy requiring users to change their password and have strong password is easy to implement in technology
  - A policy detailing what types of data can be stored where or sent to which people is much easier more difficult to implement with technology
  - Technical Solutions that are not backed by policy are prone to exploitation and workarounds
  - Often critical changes need to be approved and multiple people need to oversee the implementation of changes to reduce mistakes and ensure accountability

References

- Digitalocean - DC Security White Paper
- Cisco - Securing Enterprise Networks Whitepaper
- CCNA Materials - Cisco Certified Network Associate Certification Materials
- Network Security: Private Communication in a Public World
- cybermap.kaspersky.com
- SANS top 20
- OWASP top 10