Common threats

Threat domains

With organizations facing an ever-growing number of cyber threats, it is critical that they have robust security solutions in place.

But in order to protect themselves, organizations first need to know what vulnerabilities exist within their threat domains.

A ‘threat domain’ is considered to be **an area of control, authority or protection that attackers can exploit to gain access to a system**

Attackers can exploit systems within a domain through:

- **Direct, physical access to systems and networks**

- **wireless networking that extends beyond an organization’s boundaries**

- **bluetooth or near-field communication (NFC) devices**

- **malicious email attachments**

- **less secure elements within an organization’s supply chain**

- **an organization’s social media accounts**

- **removable media such as flash drives**

- **cloud-based applications**

Types of cyber threats

**Cyber threats can be classified into different categories.**

This allows organizations to access the likelihood of a threat occurring and understand the monetary impact of a threat so that they can prioritize their security efforts

software attacks

- **successful denial-of-service (DoS attack)** - **a computer virus**

Software errors

- **software bug**

- an **application going offline**

- a **cross-site script or illegal file server share**

Sabotage

- **authorized user successfully penatrating and compromising an organization’s primary database**

- the **defacement of an organization’s website**

Human error

- **inadvertent data entry errors**

- a **firewall misconfiguration**

Theft

- **laptops or equipment being stolen from an unlocked room**

Hardware failures

- **hard drive crashes**

Utility interruption

- **electrical power outages**

- **water damage resulting from sprinkler failure**

Natural disasters

- **severe storms**

- **earthquakes**

- **floods**

- **fire**

Internal vs external threats

Threats can originate from both within and outside of an organization.

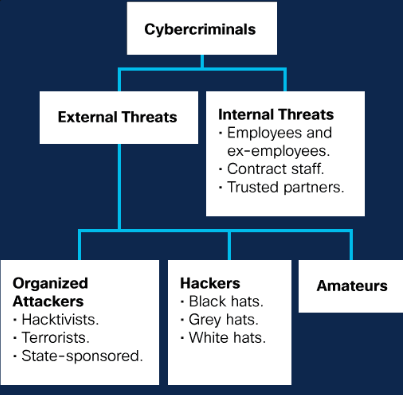
Internal threats

Are usually carried out by current or former employees and contract partners

Who **accidentally or intentionally mishandle confidential data or threaten the operations of servers or network**

External threats

Typically stems from amateur or skilled attackers who can **exploit vulnerabilities in network devices or can use social engineering techniques to gain access to an organization’s internal resources**



User threats and vulnerabilities

A user domain  
 **Includes anyone with access to an organization’s information system**, including employees, customers and contract partners.

**Users are often considered to be the weakest link in information security systems, posing a significant threat to the confidentiality, integrity, and availability of an organization’s data**.

No awareness of security

**Users must be aware of and understand an organization’s sensitive data, security policies and procedures, technologies and countermeasures that are implemented in order to protect information and information systems**.

Poorly enforced security policies

All **users must be aware of and understand an organization’s security policies**, **as well as the consequences of non-compliance**.

Data theft

**Data stolen** by users **can pose a significant financial threat to organizations**, **both in terms** of the resulting dmg to their reputation and/or the legal liability associated with the disclosure of sensitive info.

Unauthorized downloads and media

**Many network and devices infections and attacks can be traced back to users** who have downloaded unauthorized emails, photos, music, games, apps and videos to their computers, networks or storage devices, or used unauthorized media such as external hard disks and USB drivers.

Unauthorized virtual private networks (VPNs)

**VPNs can hide the theft of unauthorized information** because the encryption normally used to protect confidentiality can stop a network administrator from tracking data transmission.

Unauthorized websites

Accessing unauthorized websites **can pose a risk to a user’s data and devices, as well as the organization itself.**

Often, **these websites prompt users to download scripts or plugins that contain malicious code or adware**. **Some** of these sites can **even take over user devices like cameras and applications**.

Destruction of systems, applications or data

**The accidental or deliberate destruction or sabotage of systems, applications and data poses a serious risk to all organizations.**

**Activists, disgruntled employees or industry competitors** attempt to delete data and destroy or misconfigure devices, to make organizational data and information systems unavailable.

Threats to devices

- any **devices left powered on and unattended pose risk** of **someone gaining unauthorized access** to network resources.

- **downloading** files, photos, music or videos **from unreliable sources could lead** to the  **execution of malicious code on devices**.

- **cybercriminals often exploit security vulnerabilities within software installed on an organization’s devices to launch an attack**.

- an **organization’s information security teams must try to keep up to date** with the daily discovery of new viruses, worms and other malware that pose a threat to their devices.

- **users who insert unauthorized USB drive**s, CDs or DVDs **run the risk of introducing   
 malware, or compromising data stored on their device**.

- **Policies are in place to protect an organization’s IT infrastructure**. A **user can face** serious  **consequences for purposefully violating such policies**.

- **using outdated hardware or software** makes an organization’s **systems and data more vulnerable to attacks**.

Threats to the local area network

Local area network (LAN)

Is collection of devices, typically in the same geographic area, connected by cables or airwaver

**Because users can access an organization’s systems, applications and data from the LAN domain, it is critical that it has strong security and stringent access controls.**

Examples of threats to the LAN includes:

**- unauthorized access to wiring closets, data centers and computer rooms**

**- unauthorized acces to systems, applications and data**

**- network operating system or software vulnerabilities and updates**

**- rogue users gaining unauthorized access to wireless networks**

**- exploits of data in transit**

**- having LAN servers with different hardware or operating sys. Makes managing and troubleshooting them more difficult**

**- unauthorized network probing and port scanning**

**- misconfigured firewalls**

Threats to the private cloud

Private cloud domain includes any private servers, resources and IT infrastructure available to members of a single organization via the internet.

While many organizations feel that their data is safer in a private cloud, this domain still poses significant security threats, including:

**- Unauthorized network probing and port scanning  
 - unauthorized access to resources**

**- Router, firewall or network device operating system or software vulnerabilities**

**- router, firewall or network device configuration errors**

**- remote users accessing an organization’s infrastructure and downloading sensitive data**

Threats to the public cloud

Where a private cloud domain hosts computing resources for a single organization, the public cloud domain is the entirety of computing services hosted by a cloud, service or internet provider that are available to the public and shared across organizations.

**There are 3 models of public cloud services that organizations may choose to use.:**

Software as a service SaaS

This is a subscription-based model   
 that **provides** organizations with   
 **software** that is centrally **hosted and accessed by users via a web, app or other software**

In other words **software not stored locally but on cloud**

Platform as a service Paas

This is a subs…

**Provides** a **platform that allows an organization to develop, run and manage its applications on the service’s hardware, using tools that the service provides.**

This platform is accessed via the public cloud

Infrastructure as a service IaaS

This is a subs…

**Provides virtual computing resources such as hardware, software, servers, storage and other infrastructure components over the internet.**

An organization will buy access to them and use them via the public cloud

While **public cloud service providers** **do implement security controls to protect the cloud environment**, **organizations are responsible for protecting their own resources on the cloud**.

Therefore, some of the most common threats to the public cloud domain include:

**- Data breaches**

**- Loss or theft of intellectual property**

**- Compromised credentials or account hijackong**

**- Social engineering attacks**

**- Compliance violation**

Threatws to applications

The application domain includes: all of the critical systems, applications and data used by an organization to support operations.

Increasingly, organizations are moving applications such as email, security monitoring and database management to the public cloud.

**Common threats to applications include**:

**- someone gaining unauthorized access to data centers, computer rooms, wiring closets or systems**

**- server downtime during maintenance periods**

**- network operating system software vulnerabilities**

**- data loss**

**- client-server or web application development vulnerabilities**

Threat complexity

Software vulnerabilities occur as a result of **programming mistakes, protocol vulnerabilities or system misconfigurations.**

**Cybercriminals seek to take advantage of such vulnerabilities** and are **becoming increasingly sophisticated in their attack methods**.

An advanced persistent threat (APT)

Is a **continuous attack** that **uses elaborate espionage tactics involving multiple actors and/or sophisticated malware to gain access to and analyze a target’s  
 network**

**Attackers operate under the radar and remain undetected for a long period of time**, with potentially devastating consequences.

APTs typically target governments and high-lever organizations and are usually well- orchestrated and we;;-funded.

Algorithm attacks

**Take advantage of algorithms in a piece of legitimate software to generate unintended behaviors.**

For example, algorithms used to track and report how much energy a computer consumes can be used to select targets or trigger false alerts.

**They can also disable a computer** by forcing it to use up all its RAM or by overworking its CPU

Backdoors and rootkits

Cybercriminals also use many different types of malicious software (known as malware) to carry out their attacks

BACKDOORS

Backdoor programs, such as **netbus** and **back orifice**

Are used by cybercriminals to **gain unauthorized access** to a system **by bypassing the normal authentication procedures**.

Cybercriminals typically have **authorized users unknowingly run a remote administrative tool program (RAT) on their machine to install a backdoor** that gives the criminal administrative control over a target computer**.**

**Backdoor grant** cybercriminals **continued access to a system, even if the organization has fixed the original vulnerability** used to attack the system.

ROOTKITS

This malware is **designed to modify the operating system to create a backdoor**, which **attackers can then use to acces the computer remotely**.

Most **rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn’t be accessible and modify system files**.

Rootkits can also modify sys. Forensics and monitoring tools, making them very hard to detect. In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled

Threat intelligence and research sources

The united states computer emergency readiness team (US-CERT) and   
 the U.S. department of homeland security   
 sponsor a **dictionary of common vulnerabilities and exposures (CVE)**

**Each CVE entry contains** a **standard identifier number**, a **brief description of the security vulnerability** and **any important references to related vulnerability reports**.

The CVE list is maintained by not-for-profit, the MITRE corporation, on its public website.

The dark web

This refers to **encrypted web content that is not indexed by conventional search engines and requires specific software, authorization or configurations to access.**

Expert researchers monitor the dark web for new threat intelligence.

Indicator of compromise (IOC)

**IOCs such as malware signatures or domain names provide evidence of security breaches and details about them**

Automated indicattor sharing (AIS)

AIS, a cybersecurity and infrastructure security agency (CISA) capability,

**enables the real-time exchange of cybersecurity threat indicators**

**using a standardized and structured language called**

**structured threat information expression (STIX)** and

trusted automated exchange of intelligence information (TAXII)