Cyber Threat Management

Table of Contents

01 Introduction

02 Cyber Attacks

03 Threat Management in IX

04 Application Security Testing

05 MANRS

06 Tools & Technologies

1

Introduction

Introduction to Cyber Threat Management

Threat management refers to the process of identifying, assessing, and mitigating potential risks and dangers that could negatively impact an organization, system, or individual. This concept is particularly relevant in fields such as cybersecurity, physical security, and business continuity planning.

Types of Threats

External Threats originates outside a company, government agency, or institution

Internal Threats originates inside an organization typically by an **employee** or “**insider**”

Zero Day Threats exploits an unknown computer vulnerability

Advanced Persistent Threats (APT) is a network attack in which an unauthorized person gains access to a network and remains undetected for long times

Key Aspects

Identification of Threats
This involves recognizing potential risks or hazards that could cause harm physically, digitally or even internal.

Risk Assessment
Once threats are identified, they need to be evaluated in terms of their likelihood and potential impact. This helps prioritize which threats require the most attention and resources.

Vulnerability Assessment
This involves understanding the weaknesses or vulnerabilities that might be exploited by the identified threats.

Monitoring and Detection
Continuous monitoring of systems, networks, or environments is crucial to identify potential threats in real-time. This may involve the use of security tools, surveillance systems, or advanced analytics.

Incident Response
The incident response plan outlines the steps to take, who should be involved, and how to contain and recover from the incident.

How GT help clients?

- Vulnerability and Penetration testing
- Application Security Testing & Secure Source Code Review
- Red Teaming
- Phishing Simulation
- Network Configuration Review
- Threat Intelligence

How GT is Helping Organizations?

A
VULNERABILITY AND PENETRATION TESTING
C
RED TEAMING
B
APPLICATION SECURITY TESTING AND SECURE SOURCE CODE REVIEW

01

VULNERABILITY AND PENETRATION TESTING

By identifying and assessing potential security weaknesses in systems and networks we conduct comprehensive scans, penetration tests, and provide recommendations to mitigate vulnerabilities, helping to enhance an organization's cybersecurity defenses and reduce the risk of cyberattacks.

02

Application Security Testing & Secure Source code review

Application security testing refers to the broader category of techniques used to evaluate the security of an application by examining its behavior, functionality, and configurations. A thorough examination of a software's underlying code to uncover potential security vulnerabilities. We analyze the codebase for issues like insecure coding practices, potential exploits, and vulnerabilities that could be exploited by attackers.

03

RED TEAMING

By simulating realistic cyberattacks to evaluate an organization's security measures we employ advanced techniques to mimic the tactics of real-world threat actors, providing a comprehensive assessment of vulnerabilities and potential risks.

What is Vulnerability Assessment and Penetration Testing?

Vulnerability Assessment and Penetration Testing, is a comprehensive security testing approach aimed at identifying and addressing cyber security vulnerabilities it provides a thorough analysis to strengthen your organization's cyber security.

VA

Vulnerability Assessment
This is the initial phase of VAPT, where security professionals use automated tools and manual processes to scan and analyze for known vulnerabilities.

Benefits of VAPT

1 **Identifying Weaknesses:** VAPT helps in uncovering vulnerabilities and weaknesses in systems, networks, and applications that may be otherwise overlooked.

2 **Proactive Security:** It takes a proactive approach to security by identifying potential threats before they can be exploited by malicious actors.

3 **Realistic Testing:** Penetration testing simulates real-world attack scenarios, providing insights into how an actual attack might occur and the potential impact.

4 **Risk Mitigation:** By identifying and addressing vulnerabilities, organizations reduce the risk of security breaches, data leaks, and financial losses.

5 **Protection of Reputation:** Demonstrating a commitment to robust security through VAPT can enhance an organization's reputation and instill trust in customers, partners, and stakeholders.

PT

Penetration Testing
Following vulnerability assessment, PT simulates cyberattacks to exploit identified vulnerabilities, aiming to assess their potential impact and severity

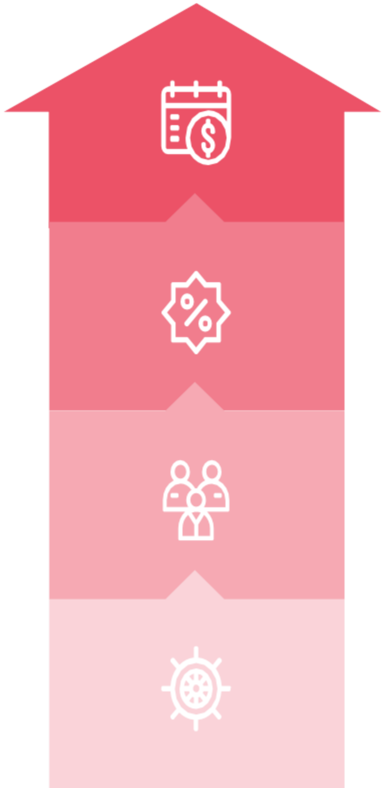
“

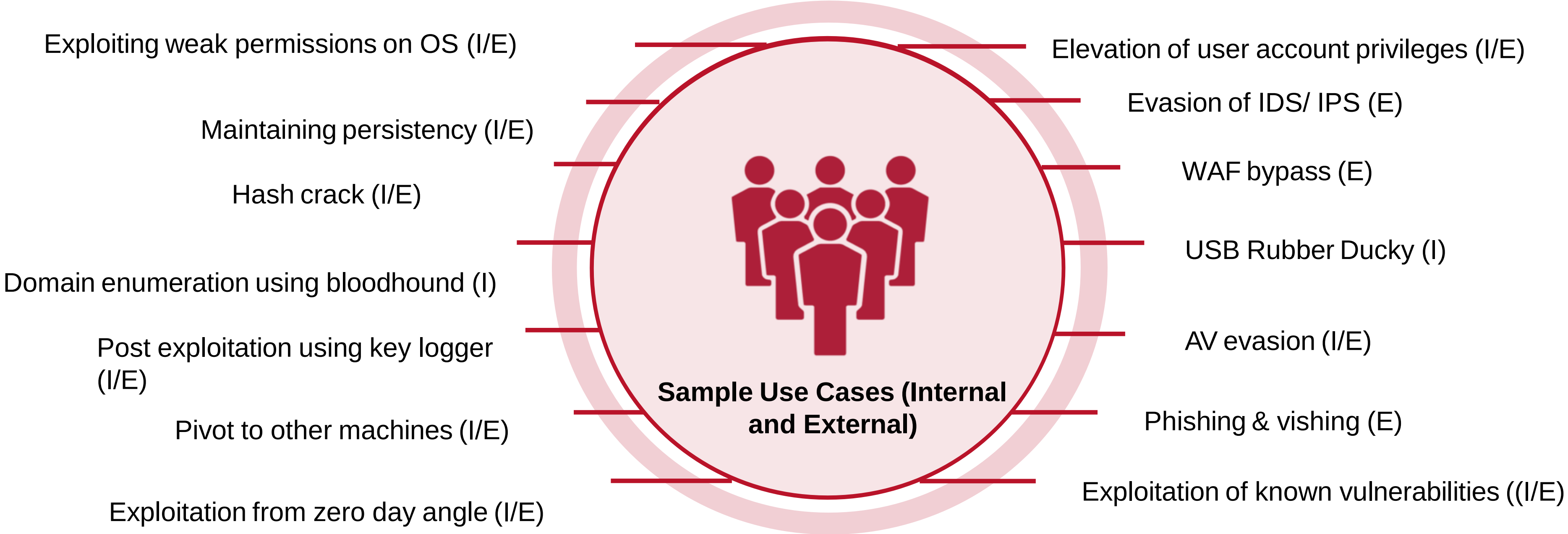
How is Red Teaming different from Penetration Testing?

”

Red Teaming

Red teaming is a cybersecurity practice in which a group of skilled professionals, known as the "red team," simulates realistic cyberattacks on a system, network, or organization. The goal is to test the security measures and preparedness of the organization's defenses.





Exploiting weak permissions on OS (I/E)

Maintaining persistency (I/E)

Hash crack (I/E)

Domain enumeration using bloodhound (I)

Post exploitation using key logger (I/E)

Pivot to other machines (I/E)

Exploitation from zero day angle (I/E)

Sample Use Cases (Internal and External)

Elevation of user account privileges (I/E)

Evasion of IDS/ IPS (E)

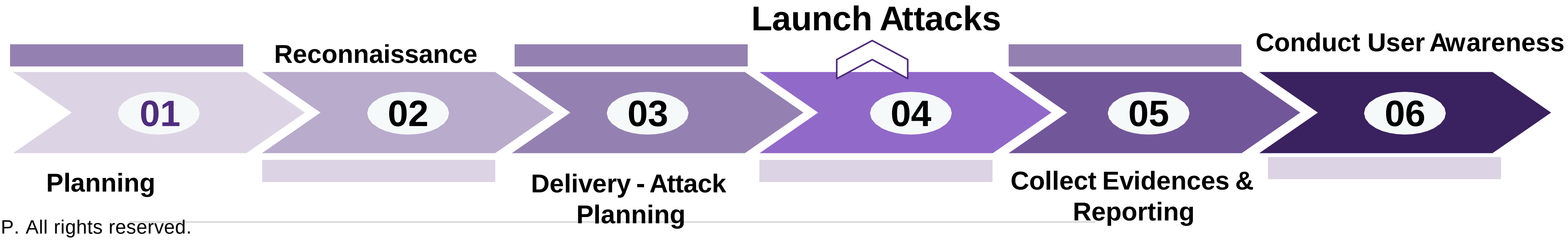
WAF bypass (E)

USB Rubber Ducky (I)

AV evasion (I/E)

Phishing & vishing (E)

Exploitation of known vulnerabilities ((I/E)



01 **Planning**

02 **Reconnaissance**

03 **Delivery - Attack Planning**

04 **Launch Attacks**

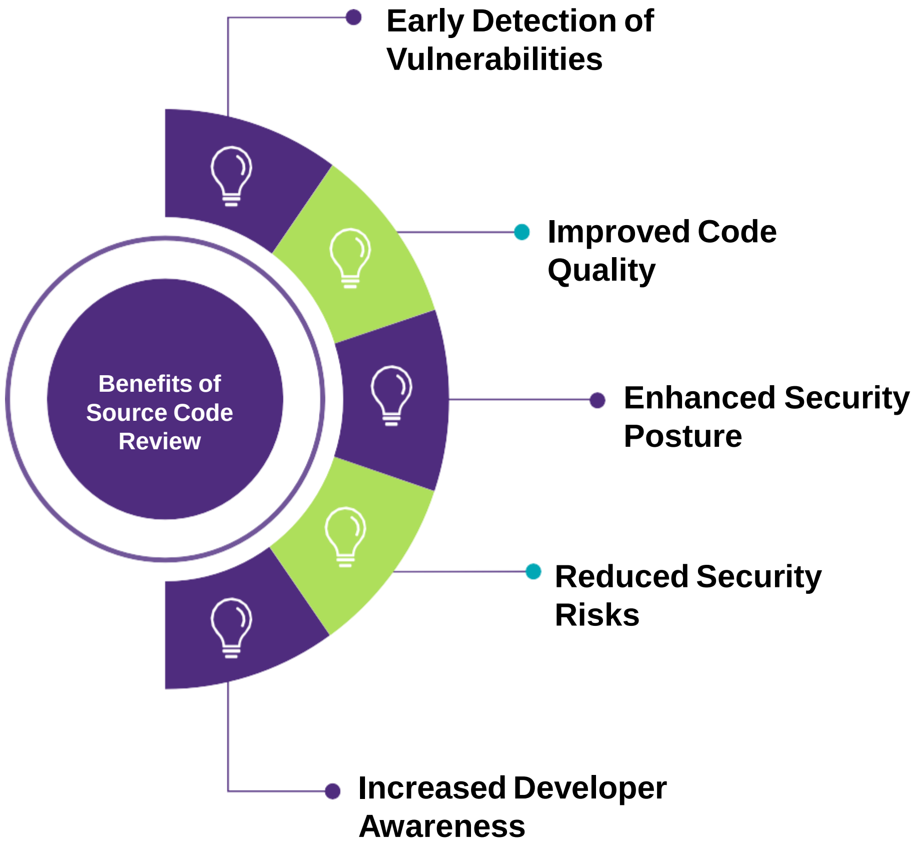
05 **Collect Evidences & Reporting**

06 **Conduct User Awareness**

Application Security Testing and Secure Source Code Review

Application Security Testing refers to the process of evaluating and assessing the security of a software application or system to identify and mitigate vulnerabilities and weaknesses that could be exploited by malicious actors.

Dynamic Application Security Testing (DAST) involves testing an application while it is running to identify vulnerabilities that can be exploited in a live environment. **Secure code review or Static Application Security Testing (SAST)** is a systematic process of analyzing source code to identify and rectify potential security vulnerabilities and weaknesses. This practice is crucial in building and maintaining secure software applications.



Benefits of Source Code Review

- **Early Detection of Vulnerabilities**
- **Improved Code Quality**
- **Enhanced Security Posture**
- **Reduced Security Risks**
- **Increased Developer Awareness**

Top 10 Most Common / Recurring Mistakes Identified in apps

Inadequate Input Validation	Poor access control mechanisms / Authorization Bypass	Malicious File Execution	Insecure Cryptographic Storage
Cross Site Scripting	Sensitive Data Transmitted Unencrypted / Insecure Communications	Reverse Engineering	Sensitive Data Exposure (Hard coded usernames and passwords)
	Obsolete / Vulnerable Software Versions	Code Tampering / Poor Client Code Quality	

Social Engineering

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Type of Social Engineering

Pretexting

It involves creating a false scenario or pretext to deceive individuals and gain their trust. Attackers might impersonate someone in authority, such as a coworker, IT technician.

Quid pro quo

In a quid pro quo attack, attackers promise a benefit or favor in exchange for specific actions or information.

Tailgating

Tailgating, also known as piggybacking, involves an attacker gaining physical access to a restricted area by following closely behind an authorized individual.

Baiting

Baiting involves offering something enticing to victims in exchange for their sensitive information or to get them to perform specific actions.

Recognizing Manipulation Techniques

To protect yourself from social engineering manipulation, it is essential to exercise caution and follow these best practices

Be skeptical of unsolicited communication or requests for sensitive information.

Be cautious about sharing personal or financial information over the phone or through electronic communication.

Recognizing Manipulation Techniques

Verify the identity of individuals through independent means (e.g., contacting them directly) before sharing information

Implement security controls such as multi-factor authentication and email filtering to mitigate social engineering risks.

Remember that awareness and critical thinking are key to detecting and avoiding social engineering attacks. If you suspect an attempted manipulation, report it to your organization's security team or the appropriate authorities.

2

Cyber Attacks

“

One single vulnerability is all an attacker needs

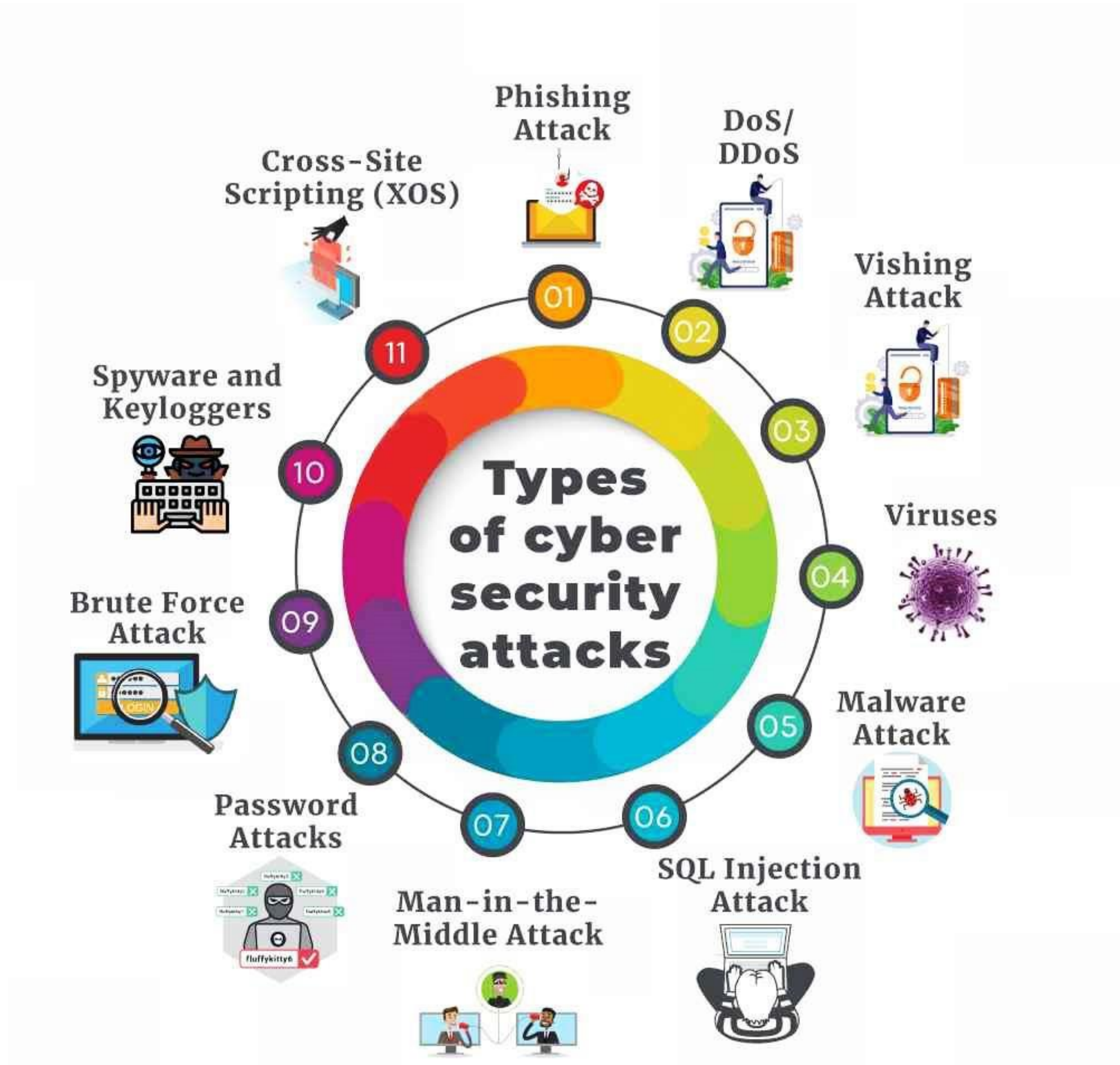
”

How do they attack?

The cyber threat landscape is constantly evolving. As cyber attackers become more skilled and organized, their attacks are becoming more sophisticated as well.

These attackers are aware of the improvements made in enterprise cybersecurity in recent years and have tailored their attacks to bypass and overcome traditional defenses.

The modern cyber attack is multi-vector and uses polymorphic code to evade detection. As a result, threat detection and response is more difficult than ever before.



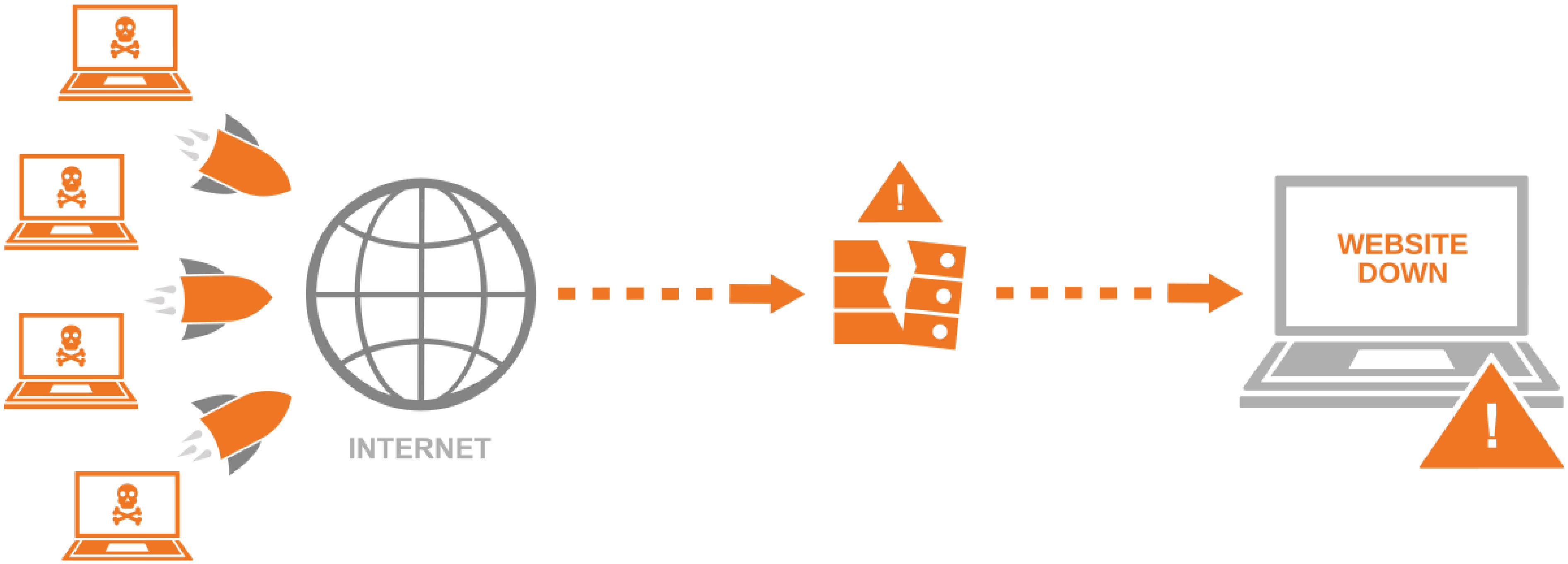
“

Let us look closer to some of these cyber attacks

”

DDoS attack

Distributed denial-of-service (DDoS) attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable.



Case Study of DDoS Attack

Background :

XYZ E- Commerce is a popular online retail platform that experiences a sudden surge in traffic and transactions during Peak shopping seasons. The website is hosted on a robust infrastructure with load balancers to ensure high availability And optimal performance.

Incident timeline :

a) Initial Surge in Traffic (Day 1):

- XYZ E-Commerce launches a promotional campaign offering significant discounts on various products.
- Cyber attackers take advantage of the increased traffic and launch a DDoS attack to overwhelm the website's servers and disrupt services.

b) Detection (Day 2):

- The IT team at XYZ E-Commerce notices a significant slowdown in website performance and receives reports from users about intermittent outages.
- Security monitoring systems detect a massive influx of traffic from various geographically dispersed sources, indicating a potential DDoS attack.

Case Study of DDoS Attack

Incident timeline :

c) Confirmation (Day 3):

- The IT team investigates the abnormal traffic patterns and confirms that it is a DDoS attack.
- The attack involves a combination of volumetric, protocol, and application layer attacks, making it challenging to mitigate.

d) Response (Day 4):

- XYZ E-Commerce activates its incident response plan and contacts its DDoS mitigation service provider.
- The mitigation service employs various techniques, such as traffic scrubbing, rate limiting, and filtering, to identify and block malicious traffic while allowing legitimate users to access the site.

e) Mitigation (Days 5-7):

- The DDoS mitigation service successfully mitigates the attack, restoring normal website functionality.
- XYZ E-Commerce communicates transparently with its customers, acknowledging the incident, and providing updates on the situation and steps taken to mitigate the attack.

Case Study of DDoS Attack

Incident timeline :

f) Post-Incident Analysis (Week 2):

- The IT and security teams conduct a thorough post-incident analysis to understand the attack vectors, identify vulnerabilities and assess the effectiveness of the mitigation measures.
- The attackers used a combination of botnets and amplification techniques, making it challenging to trace the origin of the attack.

g) Enhancements (Weeks 3-4):

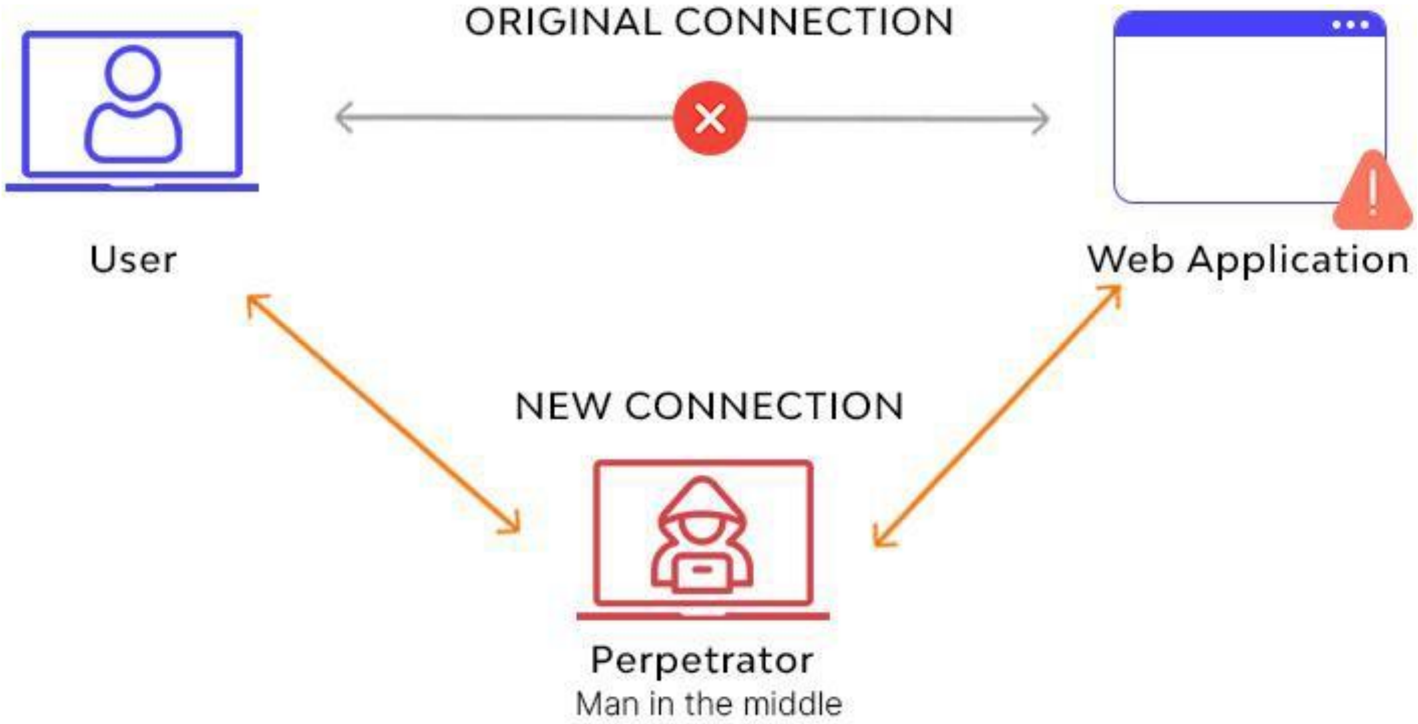
- XYZ E-Commerce collaborates with its DDoS mitigation service provider to implement additional security measures, including improved traffic monitoring, enhanced anomaly detection, and the capacity to scale mitigation efforts based on the evolving threat landscape.

h) Communication and Customer Assurance:

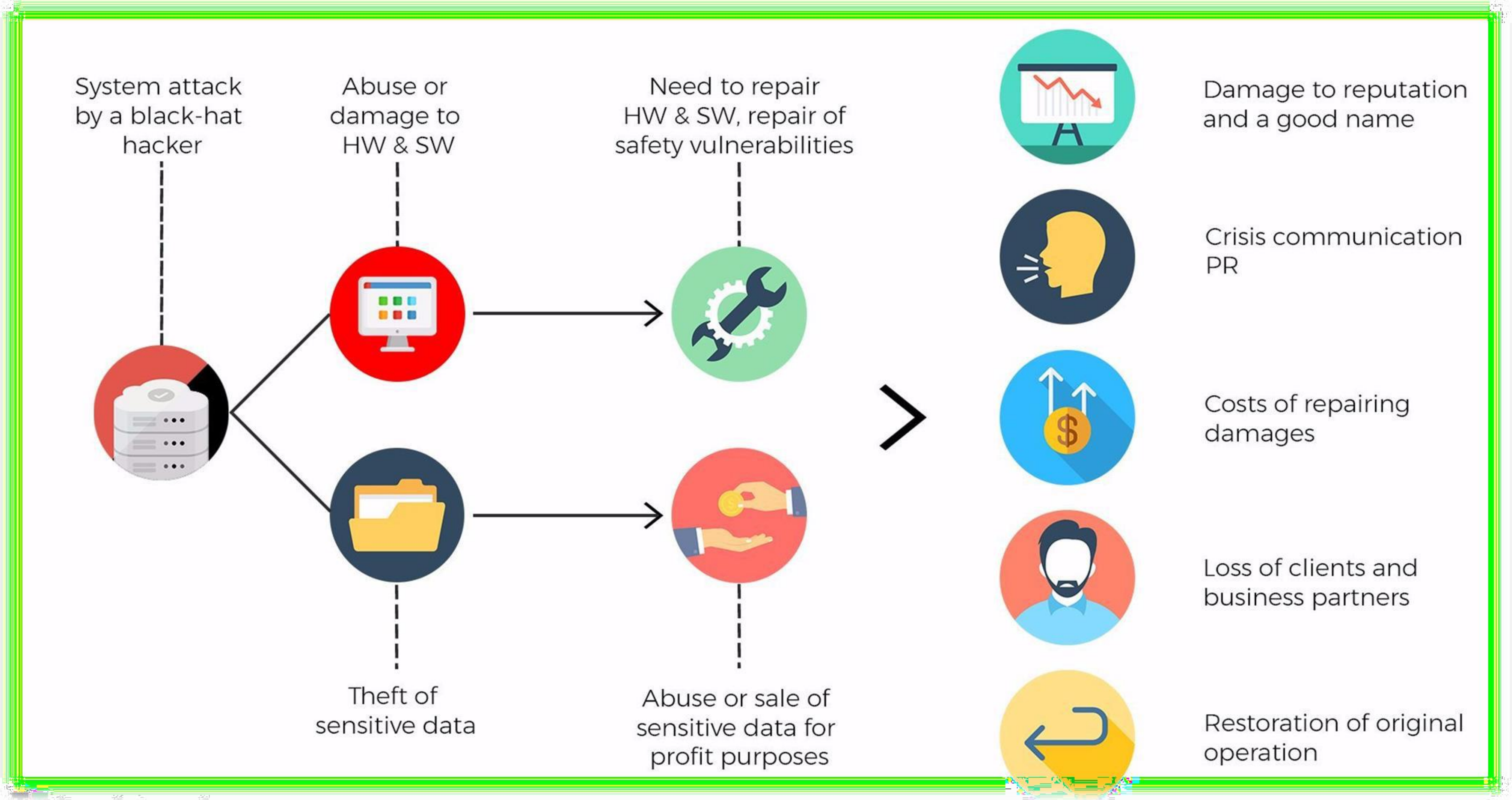
- Throughout the incident and its aftermath, XYZ E-Commerce maintains open communication with its customers through various channels, including social media, email, and the website itself.
- The company assures customers that their data remains secure and outlines steps taken to prevent future incidents.

Man-in-the-Middle attack

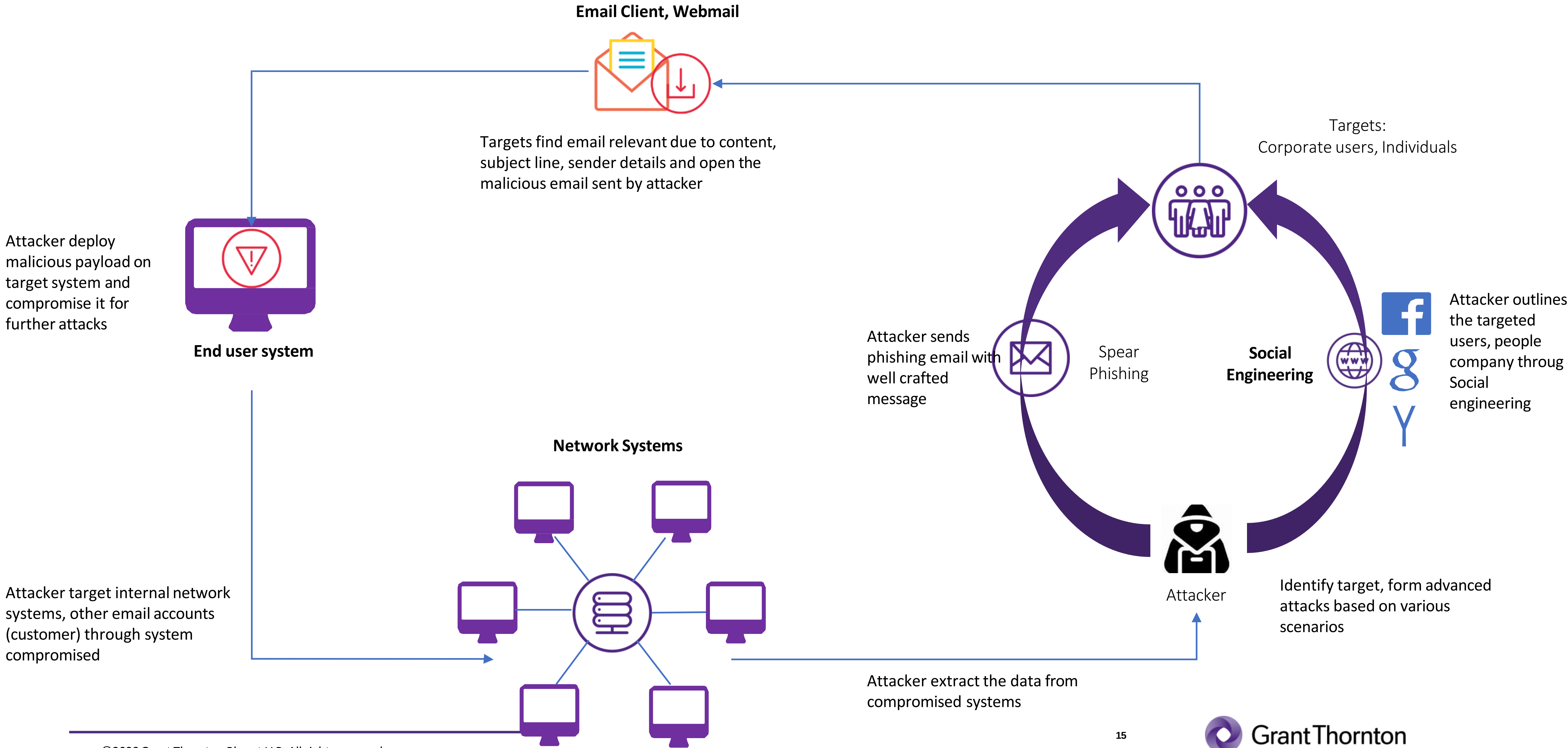
Broadly speaking, MITM attack is the equivalent of a mailman opening your bank statement, writing down your account details and then resealing the envelope and delivering it to your door.



The Aftermath


System attack by a black-hat hacker
Abuse or damage to HW & SW
Need to repair HW & SW, repair of safety vulnerabilities
Theft of sensitive data
Abuse or sale of sensitive data for profit purposes
Damage to reputation and a good name
Crisis communication PR
Costs of repairing damages
Loss of clients and business partners
Restoration of original operation

Phishing Attack Scenario



Email Client, Webmail

Targets find email relevant due to content, subject line, sender details and open the malicious email sent by attacker

Targets:
Corporate users, Individuals

Attacker deploy malicious payload on target system and compromise it for further attacks

End user system

Attacker sends phishing email with well crafted message

Spear Phishing

Social Engineering

Attacker outlines the targeted users, people company throug Social engineering

Network Systems

Attacker target internal network systems, other email accounts (customer) through system compromised

Attacker

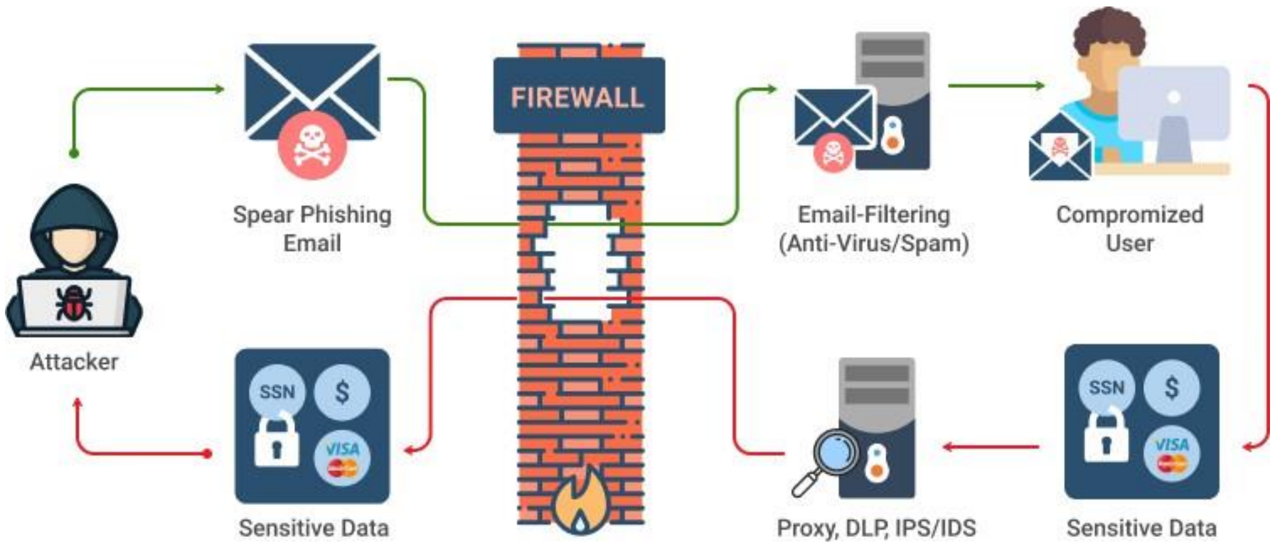
Identify target, form advanced attacks based on various scenarios

Attacker extract the data from compromised systems

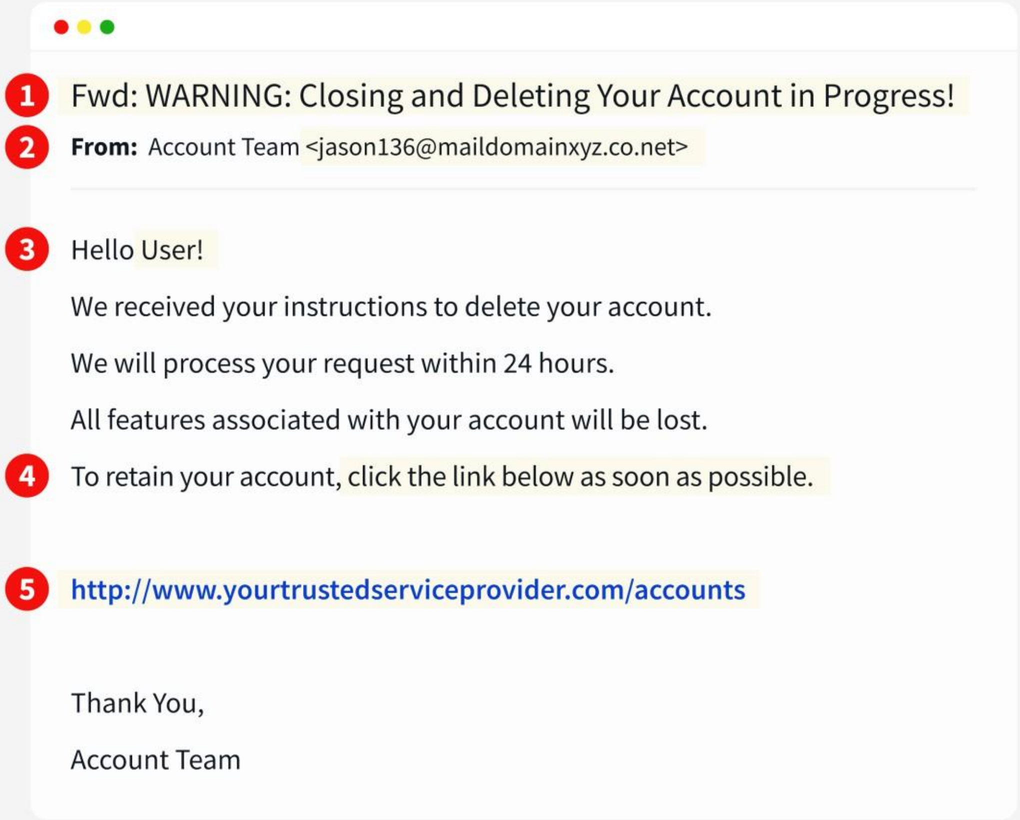
Phishing attack

How Spearphishing Works

Spear phishing messages appear to be sent from an identity - an individual or a brand - that is known and trusted by the recipient.



SIGNS OF EMAIL PHISHING



1 Fwd: WARNING: Closing and Deleting Your Account in Progress!

2 **From:** Account Team <jason136@maildomainxyz.co.net>

3 Hello User!

We received your instructions to delete your account.

We will process your request within 24 hours.

All features associated with your account will be lost.

4 To retain your account, click the link below as soon as possible.

5 http://www.yourtrustedserviceprovider.com/accounts

Thank You,

Account Team

1 **SUBJECT LINE** Sense of urgency

2 **SENDER** Legitimate sender you deem trustworthy

3 **GREETING** Generic greeting

4 **CLOSING REQUEST** A call for immediate action

5 **HYPERLINK** Statement requesting you link

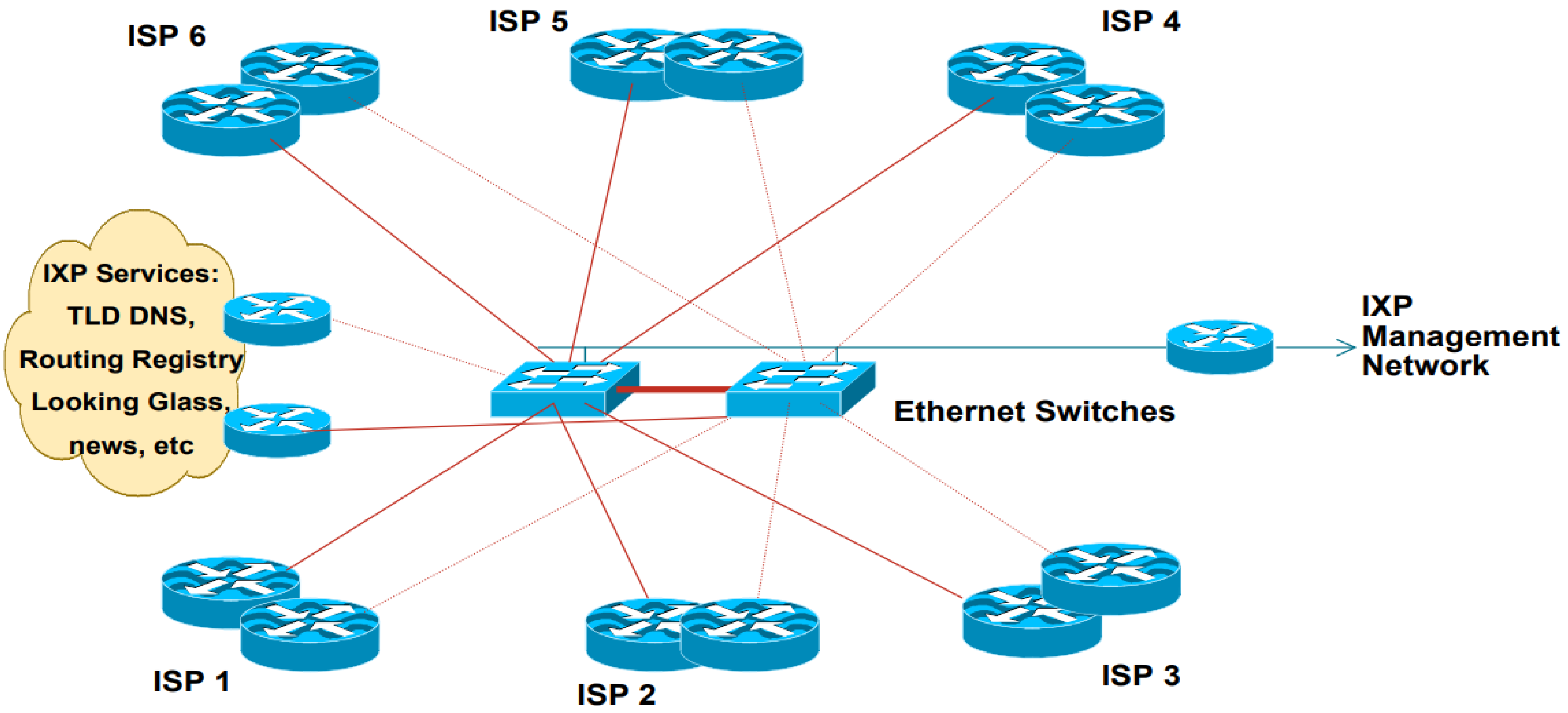
3

Threat Management in IX

Internet Exchange Points

Internet Exchange points typically comes under two categories

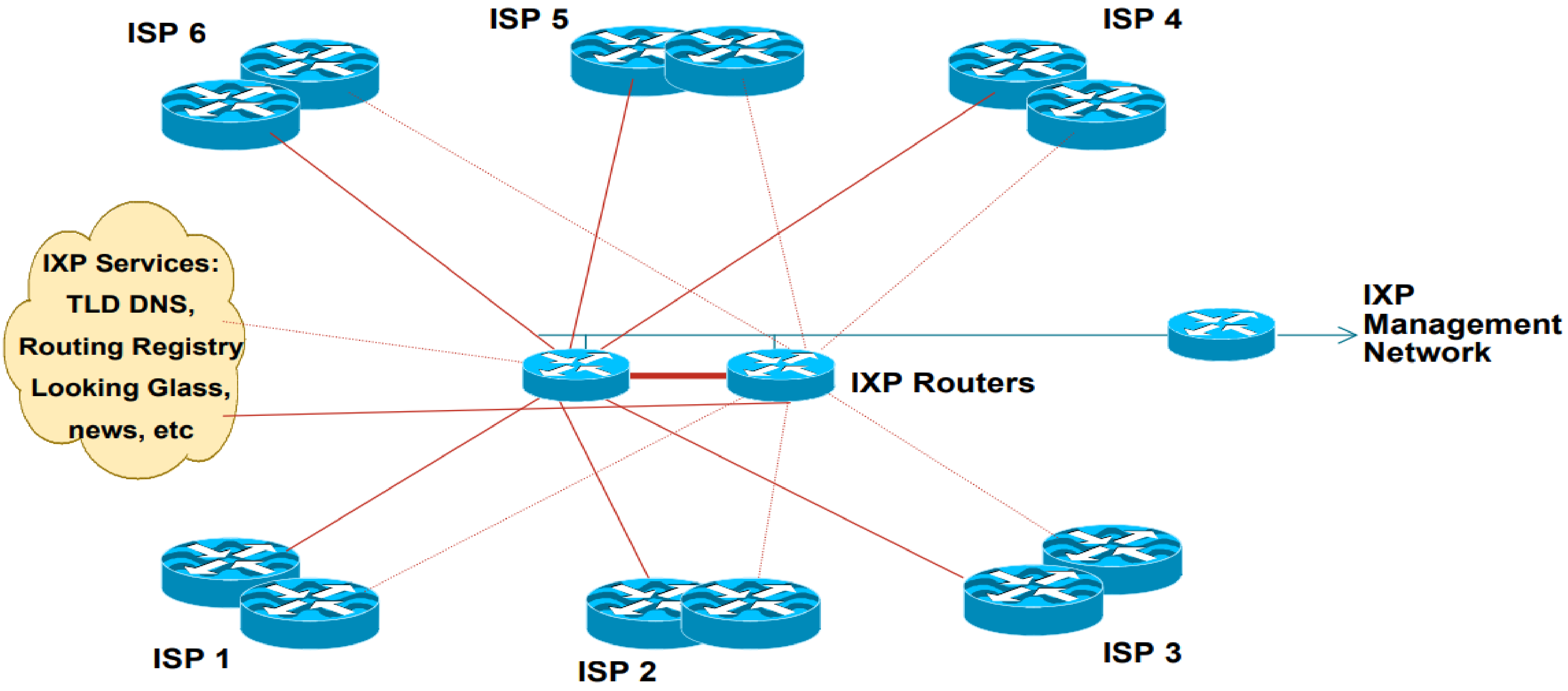
1) Layer 2 exchange point Ethernet (1000/100Mbps)



Internet Exchange Points

2) Layer 3 exchange point

Router based



Cyber Security threats in Internet Exchange Ecosystem

Like any other critical infrastructure, IXPs are susceptible to various Cyber security threats. Some of the key cybersecurity threats in the Internet Exchange Ecosystem include:

1. **Distribution Denial of Service(DDoS) Attacks:**

   As discussed in previous slides, the impact of DDoS Attacks can be overwhelming in network. It can disrupt the normal functioning of an IXP, causing packet loss, increased latency and potential service outages.

2. **Route Hijacking and Prefix Spoofing:**

   Attackers may manipulate BGP (Border Gateway Protocol) to reroute traffic through unauthorized paths or impersonate IP addresses. These attacks can lead to traffic interception, eavesdropping, or unauthorized access to sensitive information passing through the IXP.

Cyber Security threats in Internet Exchange Ecosystem

3. Malicious Route Injection:

Attackers may inject malicious routes into the BGP routing tables, diverting traffic through their infrastructure. Unauthorized route injections can lead to traffic interception, enabling attackers to eavesdrop on or manipulate the exchanged data.

4. Inadequate Security Practices:

Poorly implemented security measures, outdated software, and lack of regular security audits. Inadequate security practices can create vulnerabilities that attackers may exploit, compromising the overall security of the IXP.

Cyber Security threats mitigation in Internet Exchange Ecosystem

VAPT(Vulnerability Assessment & Penetration Testing) of Internet Exchange point Network Elements

The comprehensive features and benefits of VAPT are mentioned in Slide 6. Below are the steps which can be undertaken w.r.t IX Infrastructure

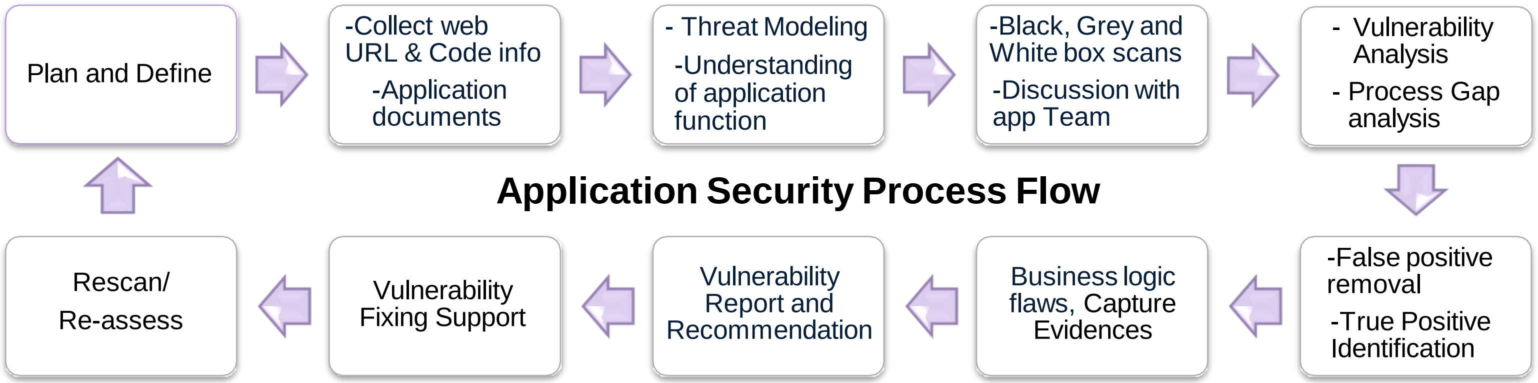
- Vulnerability Assessment of Layer 2, Layer 3 routers in Internet exchange points using Automated VA tools like Burpsuite, Nessus etc.
- Once the initial round of VA is done, a comprehensive report mentioning the detailed analysis of Critical, High, Medium and low vulnerabilities identified during testing.
- Planning of mitigating these vulnerabilities/Gaps.

Security Assessment – Dynamic and Static Applications – Web, Mobile, Thick clients, APIs

Scope Coverage

- Web Application
- Mobile Application
- Thick client applications
- Software's
- APIs
- Secure SDLC
- Threat Modeling

-Domain channel/ Process audit



Application Security Process Flow

Plan and Define

-Collect web URL & Code info
-Application documents

- Threat Modeling
-Understanding of application function

-Black, Grey and White box scans
-Discussion with app Team

- Vulnerability Analysis
- Process Gap analysis

-False positive removal
-True Positive Identification

Business logic flaws, Capture Evidences

Vulnerability Report and Recommendation

Vulnerability Fixing Support

Rescan/ Re-assess

Frequency – Quarterly / Half yearly/ Yearly / On Demand

Deliverables – Executive Summary and Detailed Technical Report with Recommendations

Security Tool

- Nmap
- Burp Suite
- Snappy Tick
- Metasploit
- MobSF
- Open source tools
- Client provided tools

Security Standards

- OWASP (Web, Mobile)
- SANS 25
- PCI DSS
- Secure coding guideline

Application Security, API Testing - Technical and Process Assessment

- Black Box and Grey Box Test with and without authentication
- Automated and Manual test, Business logic flaws
- Process review as per the application controls and documentations listed in EOI
- Revalidation test to verify closure of gaps/vulnerabilities

Source Code Review

- White box test on application code base to identify security flaws in the coding and provide recommendations
- Remove false positives, risk mapping
- Define secure coding guideline for the applications
- Create awareness of Secure SDLC by conducting training on OWASP

Mobile Application Protection

- Black box, Grey box test on the mobile application platform (iOS, Android, Windows)
- Perform reverse engineering and validate data storage check
- Test in-line with Mobile OWASP guideline
- Verify the control listed in EOI for mobile app
- Revalidate the closure post fixes

Cyber Security threats mitigation in Internet Exchange Ecosystem

Route Hijacking and Prefix Spoofing:

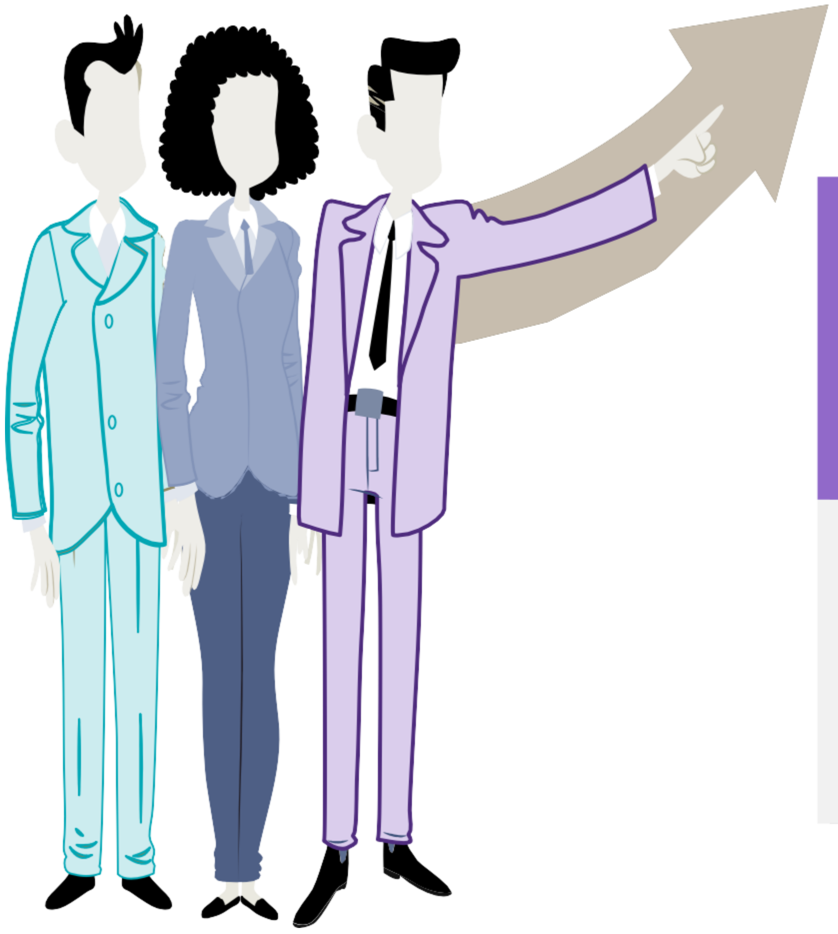
BGP Route Hijacking/Leaking, Prefix Spoofing are also some of the major vulnerabilities and occur mostly due to configuration mismanagement etc.

<u>Proactive Mitigation</u>

- Configuration analysis/check of Routers, servers can be done both manually or using automated tools like Nessus, Burpsuite etc.
- Based on configuration audit outcomes, Route hijacking and Spooking can be checked.
- The next slide mentions the Methodology of "Secure Configuration Review".

Methodology – Secure Configuration Review
Key Areas

Illustrative



Key Areas covered in secure configuration review, considering internationally recognized security best practices such as CIS and STIG benchmark

1 Operating system security review

2 Account lockout policy

3 Privilege Management

4 Audit Policy

5 User password policy

6 Patch management

7 Logging and monitoring

8 Insecure services / File system permissions

9 Network security policies

10 Network and host firewall restrictions

11 Software restrictions and application control policies

12 Secondary services and configurations

Cyber Security threats mitigation in Internet Exchange Ecosystem

MANRS(Mutually Agreed Norms for Routing Security):

MANRS is a global initiative that helps to reduce most common routing incidents. MANRS is the community initiative involving IXPs, ISPs, CDNs and Enterprise Service Providers.

Cyber Security threats mitigation in Internet Exchange Ecosystem

Why Join MANRS ?

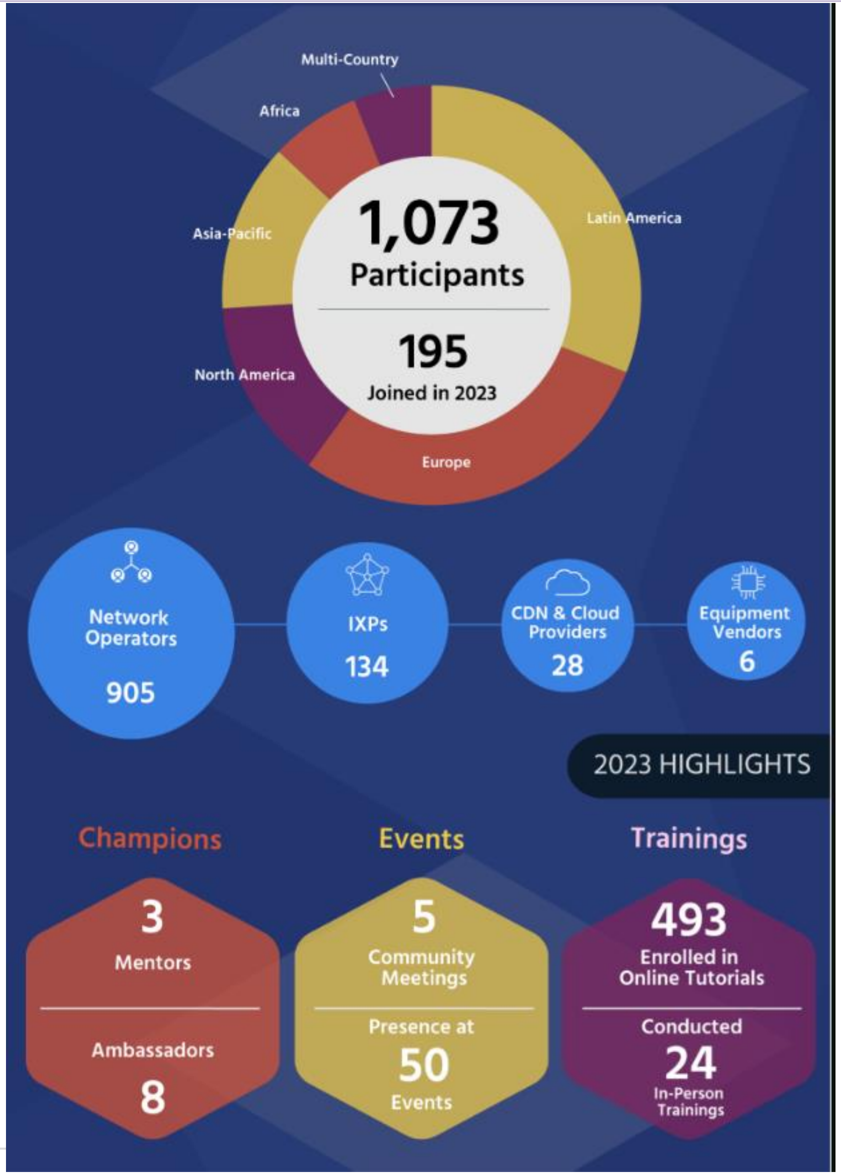
Improve security by preventing attacks and accidents

Join a community committed to a more robust and secure Internet

Lead the industry by inspiring and encouraging other operators

Cyber Security threats mitigation in Internet Exchange Ecosystem

MANRS Community Reach



Tools and Technologies

Sample Test Categories

APPLICATION SECURITY

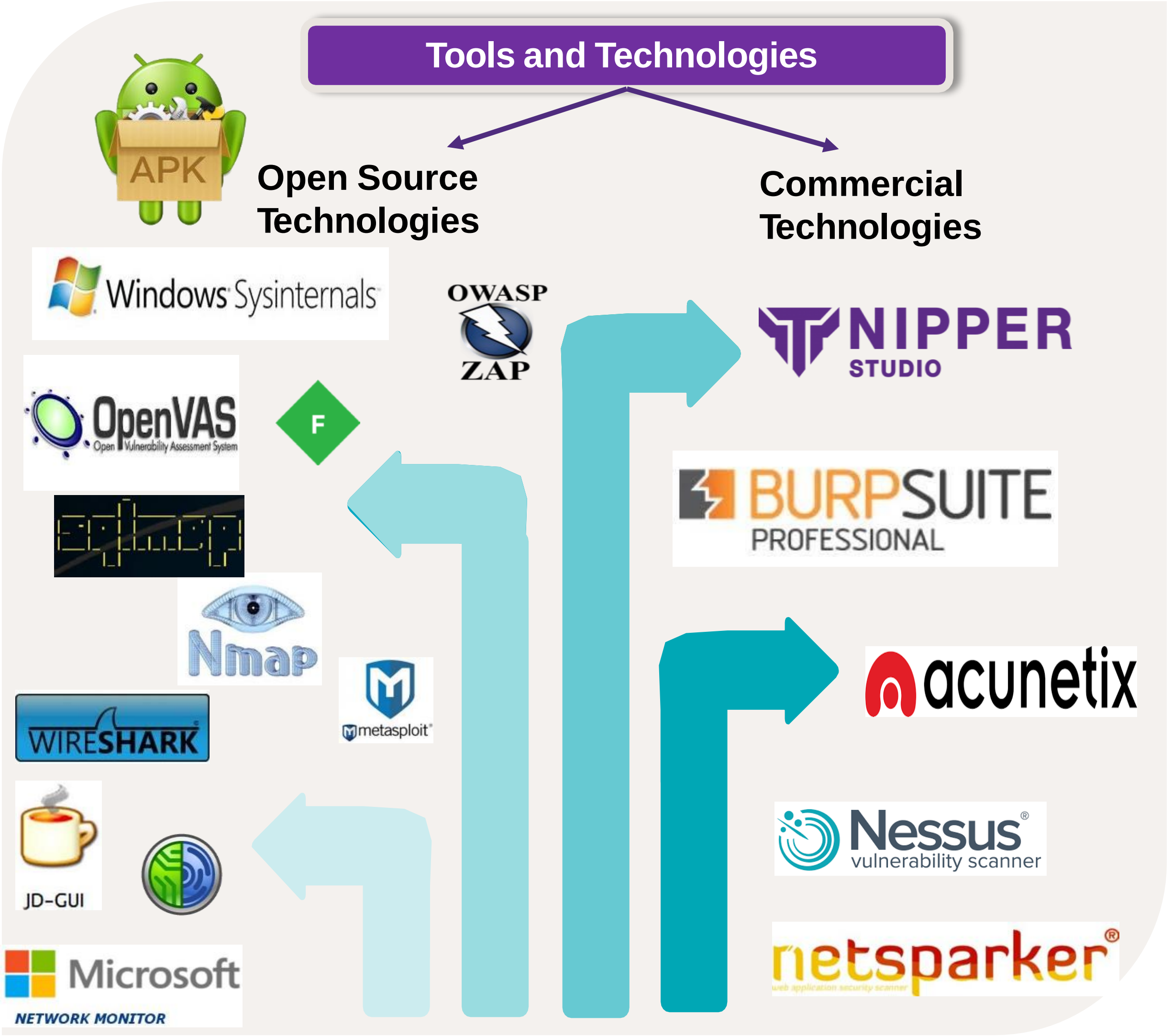
- Injections - SQL, LDAP, Code Injections, Xpath
- Broken authentication & Session related
- Cross Site Scripting
- Insecure Direct Object References
- File Inclusion Vulnerability
- Security misconfiguration
- Weak SSL or Cipher testing, Insecure Cryptographic Storage
- Bypass Multiple Factors Authentication
- Unrestricted URL Access
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components

VAPT

- Port Scanning, service enumeration
- Vulnerability scanning, controlled exploitation
- Authentication, authorization tests
- OS, DB, App and Network component tests
- Backdoor Detection
- Lockout Testing
- Password Cracking
- Default accounts and policy checks
- Database parameter checking
- Active reconnaissance
- Risk mapping as per CVSS, CWE
- Man in the middle attack

SECURE NETWORK ARCHITECTURE*

- Understanding of network flow
- Network controls for third parties
- Network controls for external networks
- VLAN segregation, Ports allowed ¥
- Rules allowed for specific application
- Review placement of firewalls and various zones
- Check for default configuration for network devices
- Response to various protocols like TCP,



Thank you!