CYBERSECURITY REPORT

INTERNSCARRER

In today's digital landscape, minor businesses are becoming main targets for cyber-attacks at a faster rate. The following report will provide an in-depth cybersecurity risk assessment for a fictional small business, called Easy Solutions Corporation. By analyzing the company's network infrastructure and identifying possible threats from an experienced attacker group known as ABC, this report aims to discover vulnerabilities and recommend robust security measures to protect the business's sensitive data and ensure operational continuity.

Example Network Setup: Easy Solutions Corporation

Network Segments:

1. **Corporate Network**

   - Servers: Web Server, Database Server, Application Server

   - Workstations: Employee PCs, Laptops

   - Network Devices: Core Switch, Access Switches

   - Security Devices: Firewall, Intrusion Detection System (IDS)

2. **DMZ (Demilitarized Zone)**

   - Public-Facing Servers: Web Server, Mail Server

   - Network Devices: DMZ Switch, Firewall

3. **Remote Access**

   - VPN Gateway: For secure remote access

   - Remote Users: Laptops, Mobile Devices

4. **Internet**

   - ISP Router: Connects the network to the Internet

5. **Guest Network**

- Guest Wi-Fi Router: Separate network for guest access

- Guest Devices: Smartphones, Tablets

Visual Diagram of Easy Solutions Corporation Network

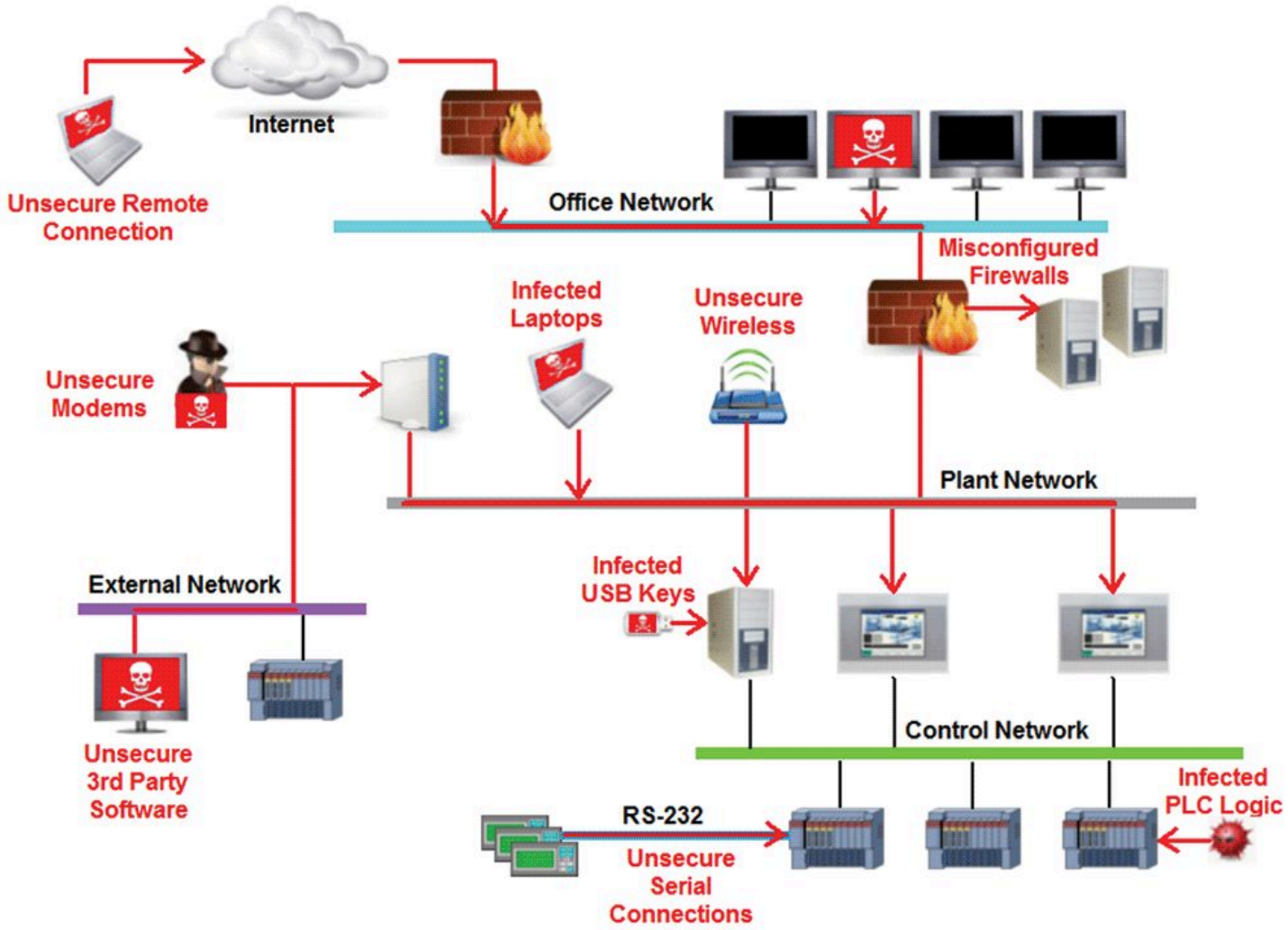


Figure 1:

Potential Threats from Attacker Group ABC

Now imagine waking up one day to find your business's sensitive data compromised and operations grinding to a halt as depicted in the above picture (figure 1). This scenario is a reality for many small businesses targeted by the likes of cybercriminal groups; in this example ABC. This group ABC, known for its sophisticated strategies, specializes in evading small business networks, stealing valuable and confidential data, and ultimately causing

operational disturbance. For Easy Solutions Corporation, understanding the threats posed by ABC is crucial to strengthening its defences and ensuring business continuity and security.

Step-by-Step Risk Assessment for XYZ Corporation

Step 1: Identify Potential Threats and Vulnerabilities

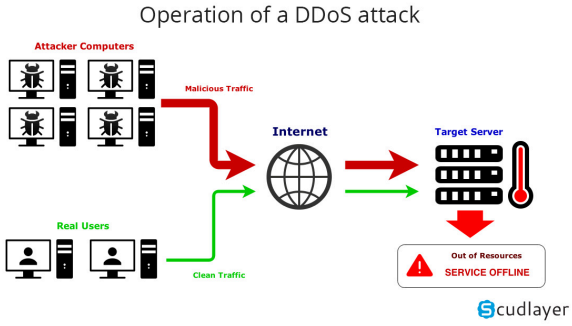
Attacker Group ABC has built its reputation in the cybercrime underworld for its effectiveness. Their method of working involves vigilantly researching their targets, identifying vulnerabilities, and executing many-sided attacks that can cripple a business within minutes. For Easy Solutions Corporation, this means facing a range of potential threats and dangers:

Phishing Attacks:

ABC excels at crafting convincing phishing emails designed to deceive employees into easily giving their login credentials or clicking on malicious links. A single successful phishing attempt can give ABC a foothold within Easy Solutions Corporation's network, leading to major data breaches.

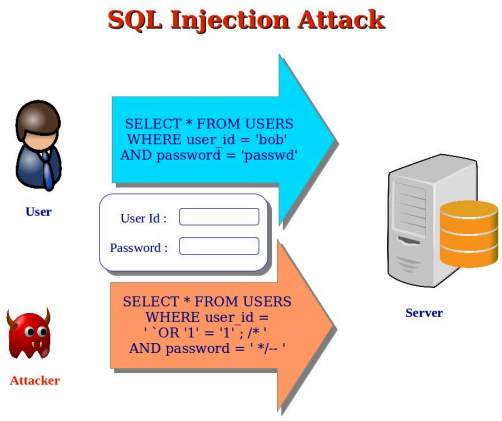
Distributed Denial of Service (DDoS) Attacks:

Public-facing servers in the DMZ, such as the company's web and mail servers, are prime targets for ABC's DDoS attacks. By overwhelming these servers with excessive traffic, ABC can render them inoperable, disrupting communications and service availability.



SQL Injection Attacks:

ABC often targets web servers with SQL injection attacks to exploit vulnerabilities in web applications. This allows them to manipulate the database server, extracting sensitive information such as customer data, financial records, and proprietary business information.



Insider Threats:

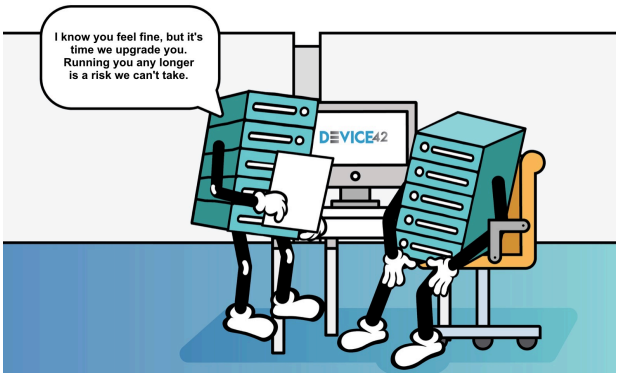
Recognizing that the greatest threats sometimes come from within, ABC may exploit disgruntled or careless employees. These insiders can accidentally or despitefully aid in compromising the company's security, providing ABC with inside access to critical systems.

Weak Passwords:

ABC leverages above-the-board password-cracking techniques to exploit weak or reused passwords. Employees using simple or predictable passwords make it easier for ABC to gain unauthorized access to sensitive systems and data.

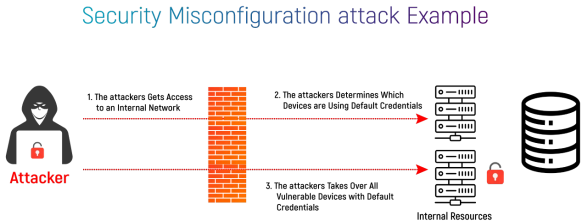
Outdated Software:

ABC continuously scans for outdated software with known vulnerabilities. Easy Solutions Corporation's servers and workstations running unpatched software become easy targets for ABC's automated exploitation tools, leading to potential system compromises.



Misconfigured Firewalls:

Firewalls are a business's first line of defence, but misconfigurations can leave gaping holes in network security. ABC is adept at finding and exploiting these weaknesses, allowing them to penetrate deeper into the network and access valuable assets.



Unsecured Wi-Fi:

The guest network at Easy Solutions Corporation might not be properly segmented from the corporate network. ABC can exploit this weakness to gain access to the corporate network through guest Wi-Fi, bypassing traditional security measures.

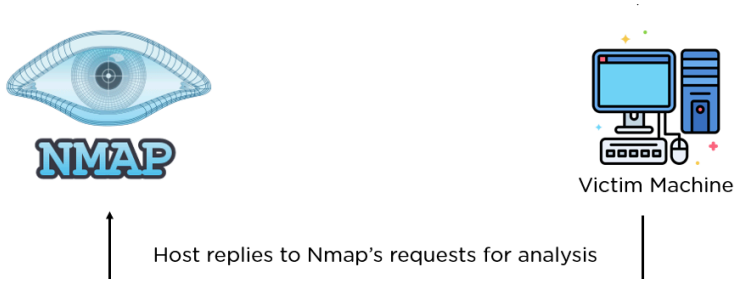
Step 2: Conduct Vulnerability Scans

Using Nmap

1. Network Mapping:

   ```bash

   nmap -sP 192.168.1.0/24




   ```

2. Service and Version Detection:

   ```bash

   nmap -sV 192.168.1.0/24

   ```

3. Vulnerability Detection:

   ```bash
   ```

```
nmap --script vuln 192.168.1.0/24
```

Using Nessus

1. Create a New Scan:

   - Target: 192.168.1.0/24

   - Template: Advanced Scan

2. Analyze Results:

   - Identify critical vulnerabilities on the web server, database server, and application server.

   - Look for outdated software and misconfigurations.

Using Wireshark

1. Capture Traffic:

   - Start Wireshark on the core switch to capture all internal network traffic.

2. Analyze Traffic:

   - Filter for suspicious activity such as repeated failed login attempts or data exfiltration attempts.

Step 3: Document Findings

1. **Summary of Findings:**

   - Phishing Attacks: Employees have received multiple phishing emails. Some have clicked on links, potentially exposing their credentials.

- DDoS Attack: The public web server experienced a high volume of traffic from a single IP, indicating a possible DDoS attempt.

- SQL Injection Vulnerability: The web server is vulnerable to SQL injection, allowing attackers to access the database server.

- Outdated Software**: Multiple servers and workstations are running outdated versions of software with known vulnerabilities.

- Misconfigured Firewall: The firewall is not properly segmenting the DMZ from the internal network, exposing internal servers.

2. Detailed Vulnerability Report:

- Critical: SQL injection vulnerability on the web server.

- High: Outdated software on the database server.

- Medium: Weak passwords on employee accounts.

- Low: Misconfigured guest Wi-Fi network.

3. Recommendations:

To protect against the relentless and sophisticated attacks of Attacker Group ABC, Easy Solutions Corporation must take decisive action. The following recommendations are designed to fortify the company's defenses and ensure resilience in the face of evolving cyber threats:

Phishing Training:

Empower Employees Against Deception: Conduct comprehensive phishing awareness training for employees. By educating staff on recognizing and avoiding phishing attempts, the company can significantly reduce the risk of credential theft and malware infections, transforming employees from potential vulnerabilities into the first line of defense.

Patch Management:

Stay Ahead of Threats: Implement a regular patch management process to ensure that all software remains up to date. By promptly addressing known vulnerabilities, the company can close security gaps before ABC can exploit them, keeping systems robust and secure.

Firewall Configuration:

Fortify Your Defenses: Review and update firewall rules to ensure proper network segmentation. A well-configured firewall acts as a formidable barrier against unauthorized access, effectively isolating sensitive internal systems from external threats and limiting the attack surface.

Password Policies:

Lock Down Access: Enforce strong password policies and implement multi-factor authentication (MFA). By requiring complex, unique passwords and additional authentication steps, the company can significantly enhance the security of user accounts, making it much more difficult for attackers to gain unauthorized access.

Network Monitoring:

Detect and Respond in Real-Time: Continuously monitor network traffic for suspicious activities. Real-time network monitoring allows the company to quickly identify and respond to potential intrusions, ensuring that any malicious activities are detected and mitigated before they can cause significant damage.

By implementing these proactive measures, Easy Solutions Corporation can build a resilient cybersecurity posture that not only deters Attacker Group ABC but also protects the company's valuable assets and ensures operational continuity. Now is the time to act decisively and fortify the defences against the ever-evolving landscape of cyber threats.

Step 4: Mitigation and Follow-Up

The battle against cyber threats doesn't end with initial defences; it's an ongoing process that requires alertness and continuous improvement. Here's how Easy Solutions Corporation can maintain a robust security posture:

Implement Remediation Measures:

Close the Gaps: Begin by applying patches to all identified vulnerabilities, reconfiguring firewalls to ensure proper segmentation, and enforcing stringent security policies. For example, if a critical SQL injection vulnerability is found on the web server, immediate updates and code reviews are necessary to eliminate this threat vector. This proactive approach prevents Attacker Group ABC from exploiting known weaknesses and significantly strengthens the network's defences.

Reassess and Verify:

Ensure Efficacy: Conduct follow-up scans to verify that all identified vulnerabilities have been mitigated. For instance, after implementing patch management and updating firewall rules, running another round of Nmap and Nessus scans can confirm that the previous vulnerabilities have been addressed. This reassessment ensures that remediation efforts are effective and that no new vulnerabilities have been introduced during the process.

Continuous Monitoring:

Stay One Step Ahead: Set up ongoing monitoring and regular assessments to detect and respond to emerging threats. For example, deploying a Security Information and Event Management (SIEM) system can provide real-time analysis of security alerts generated by applications and network hardware. Continuous monitoring ensures that any suspicious activity is promptly identified and addressed, keeping the network secure against evolving threats from ABC and other malicious entities.

Example of Continuous Improvement in Action

Consider the case of a midsize tech company that faced repeated phishing attacks targeting their employees. By conducting comprehensive phishing training sessions, implementing robust patch management, and continuously monitoring its network, the company not only reduced the number of successful phishing attempts but also significantly improved its overall security posture. Follow-up assessments showed a drastic decline in vulnerabilities, demonstrating the effectiveness of their remediation measures and ongoing vigilance.

By embracing these mitigation and follow-up steps, Easy Solutions Corporation can ensure that its defences remain strong and adaptive, ready to counteract the sophisticated tactics employed by Attacker Group ABC. The commitment to continuous improvement and proactive security measures will safeguard the company’s digital assets and ensure a secure operating environment.

Conclusion

In the realm of cybersecurity, the stakes have never been higher, and the threats have never been more misleading. For Easy Solutions Corporation, the journey to secure its network against the relentless attacks of Group ABC is not just a need—it's a strategic solution for survival and success in the digital age.