**Risk Graph**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Low** | **Medium** | **High** |
| **Web application Server** |  |  | **X** |
| **Router** |  | **X** |  |
| **Access Point** |  |  | **X** |
| **Switch** | **X** |  |  |
| **Firewall** | **X** |  |  |
| **Manuel Ip address** | **X** |  |  |

Explanation:

Firewall: I would choose a solid fire wall like Bitdefender BOX. I rated the firewall as low risk because we are using a good firewall. If the company chooses to not use a good firewall, I would raise the risk level to medium to high depending on the choice of software they want to use.

Switch: The company needs to select a good quality switch without any major security flaws.

Ip address: I would recommend changing to dynamic Ip this is not a big deal, so I ranked it as a low risk

Router Web application server: A web application server is very vulnerable to attacks from outside the company. Anybody around the world could attack the web server with various attacks so I ranked it as a high threat

Access Point: Like the web application server somebody from outside the company could attack a access point and gain access to the local servers.

**2- Flaws in the system**

**Web Application Server**

### Remote Code Execution (RCE)

### SQL Injection (SQL)

An attacker can get access to a company's systems via a persistent backdoor, leading to a long infiltration that stays unnoticed for a long time. A successful attack might result in unauthorized access to sensitive data such as credentials, credit card details, or personal user information. In recent years, the assaults have been blamed for a number of high-profile data breaches.

### Cross-site Scripting (XSS)

XSS can be used by an attacker to send a malware to an unknowing user. The end user has no way of understanding that the scripts should not be trusted, therefore he or she will run it anyhow. These coders can even change the text of an HTML page.

### Path Traversal

Path traversal attacks have the potential to access any file or directory mostly on system files, including application code or settings, as well as critical system data. A path traversal attack attempts to get access to the files and directories that aren't located in the web root folder. It's important to note that file access is restricted by system operational access control.

**Access Point**

Most companies now use web filters to limit the sorts of information that employees may access on their wired networks but safeguarding wireless networks can be more difficult. On Wi-Fi networks, controlling and monitoring access and blocking material is more difficult.

Anybody in proximity to the access point can launch an attack, particularly at public Wi-Fi hotspots where all visitor users share the same set of credentials. As a result, it's critical that measures are put in place to increase wireless access point security and protect Wi-Fi network users.

**3- You are also required to build a security policy that covers all IT infrastructure and its components, taking into consideration security awareness development.**

**IT Infrastructure Security Policy**

**Scope**

This policy applies to all users of the Firm-X's computer facilities and equipment, whether they are Firm-X-owned or leased/hired. The policy specifies what paper and electronic material belonging to the Firm-X should be protected, as well as providing guidelines on how to do so.

When a user accesses Firm-X information or computer equipment, this guideline should be followed. This policy applies to all places, including distant sites, where information in the Firm-X's possession or information processing equipment is held.

The goal of this policy is to create standards for the Firm-X's information's physical and environmental security. The level of protection required must be proportional to the amount of information kept and the dangers of unauthorized access.

The following hazards are intended to be mitigated by this policy:

• Unauthorized access to information held by the Firm-X.

• Abuse or destruction of Board information without authorization.

• The Information Commissioner's Office may impose penalty against the Firm-X or persons as a result of illegal access to protect and restricted information.

• The Firm-X or individuals may face legal action as a consequence of unlawful access to protect or restricted material.

• Damage to the Firm-X's reputation as a result of unlawful access to protect or restricted data.

**Applying the IT Infrastructure Security Policy**

* protect and restricted information must be maintained securely by information asset owners. A risk assessment should be used to determine the amount of security that should be applied to safeguard the data being kept.
* The Firm-Xs must guarantee that the type of information and equipment held in their facilities has adequate control measures in place.
* Physical access to buildings should be limited to permitted personnel and access to secure sections should be tightly regulated. Personnel working in secure locations should question anyone who isn't carrying a badge or other form of identification. Each team is responsible for securely securing doors and windows.
* Identify and access tools/passes must be kept by officers who are authorized to enter such places and should not be given or distributed to anyone.
* Visitors to secure areas must sign in and out, indicating their arrival and departure times, and must wear an identity badge. At all times, an ICT Services employee must keep an eye on all visitors who enter protected ICT locations.
* ICT Services shall ensure that keys to all secure spaces containing ICT equipment are kept safe and are not kept close to these secure areas.

**Equipment Maintenance**

ICT Services and users are responsible for ensuring that all of the Firm-X's ICT equipment is maintained in line with the manufacturer's instructions and any established internal processes to ensure that it stays in working condition. The ICT Service Desk will perform the following tasks:

• Make a copy of all manufacturer's instructions and keep them safe.

• Make sure that only authorized experts operate on the equipment.

• Keep a detailed record of any corrective work done.

• Determine if any insurance coverage is required.

• Keep track of any errors that occur and the measures that must be taken.

The ICT Customer Service will keep track of equipment's service history so that when it becomes obsolete, choices may be made about when it should be replaced.

**4- Provide your recommendations to mitigate the identified flaws.**

**RCE:**

Since the chain of execution to effect entry can differ so much, RCE attacks are difficult to prevent. To reduce the number of vulnerabilities in your environment, patch and update all of your software as soon as possible. Unfortunately, most attackers take a list of the most recently discovered vulnerabilities and happily exploit them, knowing full well that most organizations have failed to apply the required updates and mitigation patches. Threat actors, on the other hand, are able to exploit old vulnerabilities that have remained unpatched for years.

**SQL injection:**

The majority of SQL injection attacks may be prevented by using parameterized queries. The query string always has to be a hard-coded constant that does not include any dynamic data from any source. Don't make a case-by-case decision about whether or not a bit of data is reliable. Continue to utilise string combining within the query for situations that are considered safe.

**XSS:**

Depending on the intricacy of an app's code and how it manages user-controllable data, limiting cross-site scripting (XSS) might be tough. In general, preventing XSS flaws will almost definitely need a combination of multiple measures:

1. filter the data. Filter as strictly as possible based on expected or valid input at the point where user input is received.
2. Data on the output should be encoded. Encode user-controllable data in HTTP responses to avoid it being misinterpreted as active content. This may necessitate a combination of HTML, URL, JavaScript, and CSS encoding, depending on the output context.
3. Use response headers that are appropriate. You can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret HTTP responses in the way you intend, preventing XSS in HTTP responses that aren't supposed to contain any HTML or JavaScript.
4. Policy for Content Security. You can utilize Content Security Policy (CSP) as a last line of defense to mitigate the severity of any remaining XSS issues.

**Access point:**

A web filtering solution is a simple method to increase wireless access point security. Businesses often use web filtering solutions to safeguard wired networks, but there are other options available to increase wireless access point security.

A web filter acts as a barrier between network users and the Internet. Users can be prevented from viewing harmful, unlawful, or inappropriate online content by using controls. Even if each user has their own set of access rules, without a web filter, users will be subject to malware and phishing efforts, and the hotspot provider may be held accountable for unlawful activity on the Wi-Fi network.

To increase wireless access point security, there are two techniques to implement Wi-Fi web filtering. One option is to utilize a list of classified domain names to manage content. The other is DNS-layer web filtering, which makes use of the DNS lookup procedure that must occur before a user is sent to a website after typing the domain name into their browser. To allow the web page to be located, the DNS server converts the domain name into an IP address.

**Path Traversal**

* When employing file system calls, prefer to work without human input.
* Make sure the user can't give the entire route by enclosing it in your path code.
* Validate the user's input by allowing only known valid data and not sanitizing it.
* To limit where the files may be retrieved or saved, use chrooted jails and code access policies.
* If you have no choice but to utilize user input for file operations, make sure to normalize it before utilizing it in file IO APIs.

$

<https://www.bugcrowd.com/glossary/remote-code-execution-rce/>

<https://portswigger.net/web-security/sql-injection>

<https://owasp.org/www-community/attacks/xss/>

[https://portswigger.net/web-security/cross-site-scripting/preventing n](https://portswigger.net/web-security/cross-site-scripting/preventing%20n)