Security Infrastructure Design Document for John Doe IT Development Company

This is a security infrastructure document for the aforementioned company and seeks to address security concerns in several areas:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

Introduction:

Security of an organization's IT infrastructure is very important to both the organization and its customers. It will help to improve their service delivery and most importantly improve trust and gain more customers in the process. I will not be using a layered approach to recommending the security process and steps but rather will be applying these elements to the various areas of concern/interest requested by your company:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rules recommendations
- Wireless security
- VLAN configuration recommendations
- Laptop security configuration

- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

Intended Audience:
John Doe IT Development Company and other small to medium sized organizations looking to improve their security process and implementation.

Recommendations:

1.) **An external website permitting users to browse and purchase widgets**:

External Website Security and Authentication System:

To secure your customer data the following is recommended:-

A.) Universal Second Factor (U2F)

a) This is a standard developed jointly by Google, Yubico and NXP Semiconductors and incorporates a "challenge-response mechanism", along with a public key cryptography to implement a more secure and more convenient second-factor authentication solution. This is an improvement over the old OTP mechanism. The interactive nature of the process ensures that customers are protected against "phishing attacks".

B.) OAuth, Authorization system:

a) This is addition to the above U2F system will ensure that only authenticated will be given access to the data that they are authorized to view or modify.

2.) **An internal intranet website for employees to use**:

Internal website security recommendations:

A.) Active Directory (AD) can be used to authenticate and authorize employee access to the company intranet. This is an affordable solution for small organizations.

3.) **Secure remote access for engineering employees:**

Remote access solution:-

A.) Virtual Private Network (VPN), this can be used to create secure communication channels for the engineering team members. This will provide a secure encrypted channel for communication with company network services.

B.) Proxy Servers can also be used to provide secure remote access to company resources and services. This configuration can be used for logging web requests of client devices. The devices can be used for logs, and traffic analysis, and forensic

investigation. The proxy server can be configured to block content that might be malicious, dangerous, or just against company policy.

C.) Reverse proxy server can be used also to provide secure connection.

D.) It's good practice to keep the network that VPN clients connected to separate using both subnetting and VLANs. This gives you more flexibility to enforce security on these VPN clients. It also lets you build additional layers of defenses,

4.) **Reasonable, basic firewall rules:**

Firewall and basic rules recommendations:-

I would recommend the use of the “implicit denial” firewall rule. This will ensures that any required service access will be explicitly granted and all other services will be denied access. This promotes a culture of “grant access on per need basis”. Firewall configuration should be applied at two levels”:

1.) Network level: protects against malicious traffic into the network

2.) Host-based level: this provides another layer of security and ensure each device is individually protected even when follow peer devices are compromised.

5.) **Wireless Coverage in the Office:**

Wireless Security:

WPA2 with AES/CCMP mode is the next best option and to protect against brute force or rainbow table attacks, a long and complex passphrase should be used that wouldn't be found in a dictionary would increase the amount of time and resources an attacker would need to break the passphrase. Changing the SSID to something uncommon and unique, would also make rainbow tables attack less likely. The other option would be 802.1X with EAP-TLS. But this is extremely complex to setup so the former will do.

6.) **Reasonably Secure Configurations for Laptops:**

Laptop Security Configurations:

The recommendations would be

A.) Full disk encryption (FDE) should be utilized to ensure that if any device gets stolen access to the hard disk will be difficult. And a recovery password or escrew key functionality will ensure that if a staff forgot their it can be recovered by the system admin.

B.) Using AD (Active Directory Group Policies) the password format can be enforced which should be a password with the following characteristics:

a) Complex with both symbols, alpha and non-alphanumeric characters

b) Password expiration, this forces the staff to change their password periodically (but the expiration period should be evenly spaced to avoid encouraging written down passwords).

C.) Host-based firewall to add another security layer and help protect the device from compromised peer devices.

D.) Use of company recommended antimalware software.

7.) **Other recommendations:**

1.) **Application Policy Recommendations:**

a) What software are allowed on company machines.

b) Company software update process and procedure.

c) Trusted browser plugins and addins and their potential risk and how to handle them.

d) Complete ban on file sharing software and pirated software use on company devices.

e) Made available to all company staff via the the document server.

f) Only trusted software vendors are recommended.

2.) **Security and Privacy Recommendations:**

a) Only staff authorized to have access to user data should be granted access

b) Customer data should never be moved from location without authorization and using so called mobile storage devices, if these device most be used to move data, then

only recommended media should be used and an encryption mechanism must be applied.

c) Unauthorized sharing of customer information is to be discouraged and enforced at all levels.

d) The legal implications of handling customer data must be reviewed and adhered to.

3.) **Intrusion detection or prevention for systems containing customer data:**

Intrusion detection:

1.) Centralized logging using tools like Wireshark to log network activities and analysis

2.) Periodic system audits

Intrusion Prevention:

1.) Use of Network and host level firewalls

2.) Threat Modeling

3.) Periodic vulnerability scanning of the network using tools like OpenVas etc.