**Security Infrastructure Design Document**

**Introduction**

This document describes the design goals in accordance with the requirements, by providing a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine scenarios in terms of interaction and operation. The high-level system design is further decomposed into low-level detailed design specifications including hardware, software, data storage and retrieval mechanisms and external interfaces.

**Document Purpose**

The Security Infrastructure Design Document helps to document and track the necessary information required to effectively define architecture and system design in order to give the guidance on the security architecture of the IT environment that is going to be established.

1. **General Overview**
2. **General Overview of Services**

The company requires an IT infrastructure to perform their business activities that involves e-commerce applications and external website. The company also requires access to internal website along with remote command-line access for their employee to the workstations.

1. **List of Security Measures Related to Services**

**The following are the key considerations associated with the security of the infrastructure:**

* 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

1. **Risks**

Since the infrastructure is meant to carry out the e-commerce related transactions that may involve third party merchant authorizations and financial related issues, a strict security mechanism needs to be enforced so as to ensure that there is no such issue related in customer transactions as it may affect the reputation of the organization.

Additionally, there should be a backup mechanism to take the data backups at regular intervals to deal with any unwanted situations like system failures, attacks by intruders, etc.

1. **Design Consideration**
2. **Goals**

**The following are the desirable outcomes of the security infrastructures proposed to be implemented in the organization:**

* 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

1. **Architectural Strategies**
2. **External Website to Perform Browse and Purchase Activities by Customers**

In order to provide a secure e-commerce transaction, the following are the primary which security goals include:

* Protecting confidentiality of the data
* Making sure that unauthorized persons or systems cannot access the information of users
* Making sure that the information accessed is genuine
* Making the data accessible and usable
* Logging the transactions for further reference and support activity
* Verifying the authenticity of a person to perform a transaction

Data confidentiality can be achieved by using HTTPS instead HTTP on the external website, which will encrypt all communications and data between client and the server.

As for authenticating and authorization regardless of any data can be achieved by using two-factor authentication, which include OTP protocol in every transaction the customer made.

1. **Intranet Website Accessed by Employees**

Since the data is accessed by the company employees, it should only be available to company’s level of access. The following are the considerations in this case:

* Making sure that the access is within their intranet by implementing a firewall mechanism
* Specifying the authentication mechanism to access the website by the employees
* Supervising the activities and user management on the website by an administrator

This can be achieved by having a good security policies and using access management tools, which restrict some resources to be accessed only for the authorized party.

Using configuration management tools like puppet also can improve the company internal security by maintaining some strict requirements on the applications and systems that can be used in the company machines

1. **Secure Remote Access for Engineering Employee**

We can perform safe implementation of remote access control objectives based on the following security considerations:

* Develop a Cybersecurity Policy for Remote Workers

To ensure the safety of our network we need to have a strict policy about remote access, such policy can be made upon answering some questions like this:

* What device is allowed for remote access? Is it company-owned devices or personal devices?
* What type of data can be accessed remotely?
* What kind of services can be accessed?
* What type of authorization does it have?
* etc
* Virtual Private Network (VPN)

A virtual private network is software that creates secure connections over the internet by encrypting data. Through the process of tunneling protocols to encrypt and decrypt messages from sender to receiver, remote workers can protect their data transmissions from external parties.

* Two-Factor Authentication

Two-factor authentication can be included to improve remote access security by using two different types of authentication procedure.

1. **Basic Firewall Rules**

For services that the company needs we can use Whitelist rules, which make only the services that are in list and trusted can be accessed.

1. **Wireless Coverage in the Office**

We can use the newest protocol such as 802.11 WPA2 adapter/router with PSK(pre-shared key) configuration or a login based limited access to company WIFI by the employees

1. **V-Lan Configuration**

VLAN network segmentation creates security zones that enables flexible and strong control of what a remote user can access. security zones separating incoming traffic from internal resources. Using dynamic VLAN assignments and access control lists, we can control user access based on the conditions

1. **Laptop Security Configuration**

One of the most vulnerable parts of the infrastructure is the laptop computers that employees use. These devices can be responsible for bringing in viruses or malware or causing the organization to lose sensitive data. This can be checked using the techniques such as:

* Encrypting the disks on the laptops
* Ensuring Antimalware/Antivirus are up to date in regular intervals
* White listing the devices on the network
* Running a product such as System Center Configuration Manager, LANDesk, Altiris, or some other systems management platform

1. **Application Policy Recommendation**

Defining a good application policy can be achieved by considering some aspects, like this:

* Integrate secure coding principles in all software components of infrastructure.
* Perform automated application security testing as part of the overall application testing process.
* Development and testing environments should redact all sensitive data or use de-identified data.
* Compliance with industry standard data policies and protocols

As for maintaining the policies in the machine company, we can used configuration management tools such as puppet to monitor all the machine in the company.

1. **Security and Privacy Policy Recommendations**

* Explain How the organization Collects and Use Personal Information:
  + Cookie Policy – Cookies are used to store user preferences or shopping cart contents. Clearly explain your cookie practice.
  + How organization will Share Customer Information – Customers need to know that their data will only be used to complete the transaction and that any further use of that data (including selling or distributing it) requires their consent.
  + Contact Information – Make it easy for your customers to contact you or file a complaint.
* Display Privacy Policy: Make sure new customers or users have easy access to your policy mandatorily
* Publish Email Opt-Out Policies: Include opt-out options in your email marketing
* Get a Seal of Approval: Third party validation of your online privacy and security policy can enhance your credibility. And trust of security

1. **Intrusion Detection or Prevention for Systems Containing Customer Data**

As the demand for E-Commerce grows on the Internet so will the increasing potential for E-Commerce sites to be attacked. Implementing security methodologies pertaining to an E-Commerce environment is not a simple thing. It should consider various threats and anomalies that can cause an attack. This can be achieved through penetration testing and reverse engineering to detect by signature or by an anomaly. This can be achieved by a third-party IDS system readily available in the market

1. **Summary**

Thus, we can conclude the report of the security infrastructure of the organization has been assessed and recommendations were made as required for the proposed environment as specified

1. Key assets being protected:

* Customer information
* Company related information

1. Key threats to protect against:

* Intrusion to website
* Data Loss

1. Key activities to protect against:

* Customer purchase of artifacts
* Payment transactions
* Employee data