Ravi Patel

Nimbus (eCommerce Application) — RISK ASSESSMENT

Summary

This is a security risk assessment tailored for the Nimbus company — its digital and physical operations. We have concluded that there is minimal risk to the company as long as they are aware of threats and have taken all measures to reduce security risks. Keeping information local rather than on cloud servers would be a great benefit to the company, to keep the amount of people who have access to their data at a minimum. Customer information is important over all else, and administrators must work to ensure that vulnerabilities are kept to a minimum, especially in regards to the consumer.

ASSESSMENT

1. Introduction

1. Purpose

Overall, the security requirements of Nimbus & co are minimal, but necessary due to the data that will be stored — namely customer and employee information, product information, and payment information related to purchasing and selling of goods on the Nimbus website.

1.2. Scope of this risk assessment

This risk assessment will include elements of the website, users, employees, and server locations. Ideally, this server would be completely local but due to ease-of-use and project requirements, Nimbus will be using a cloud-based infrastructure for its operations.

2. Risk Assessment Approach

2.1 Participants

Participant
Ravi Patel — admin of CMS installed on Azure
Ravi Patel — admin of Azure account that hosts the website
[Censored] — admin
[Censored] — admin
[Censored] — admin

2.2 Techniques Used

Technique	Description

Cost-benefit Analysis	Thinking about how we would or would not benefit from additional security helps in understanding Nimbus's overall need for security
Threat Vulnerabilities	Thinking about potential vulnerabilities is a good way to secure a system proactively.
Risk Mitigation	Although cloud services are inherently risky compared to local servers, we will be taking that risk after doing a cost-benefit analysis and due to the ease-of-use of cloud-based servers.

2.3 Risk Model

Refer to NIST publication SP-800-30

3. System Characterization

3.1 Technology components

Component	Description
Applications	WordPress CMS
Databases	Azure's Back-end database system
Operating Systems	Running on a PHP-based system
Networks	A cloud network hosting a website using a pre-built CMS

3.2 Physical Location(s)

Location	Description
MSU	This is the location that we will be conducting most of our web-based development, and thus the building internet must be secure and proactive in preventing all attacks.
Micosoft Azure	The physical location where microsoft azure web servers are located, this is a fundamental piece of any risk assessment because rather than using local servers in one place, there is a third party that has the potential ability to access our data.

3.3 Data Used By System

Data	Description
Credit Card Numbers	Credit card numbers are important and must be kept secure (using an SSL would be handy, but may not be applicable in the scope of this project)
Customer Information	Customer information such as shipping information is also vital information that must be kept private from prying eyes
Employee Logins	Employee login information to access and edit the website and web-store must be secure and kept confidential at all times so as to not increase risk
Product Information	Product information is less vital but still important, there may be figures in the final admin page that is not publicly viewable and these numbers should stay on a private page rather than a public page.

3.4 Users

Users	Description
Customers	Customers would create an account and login using WordPress e-commerce plugin
Administrators	Administrators would login using their assigned login information, this must be kept confidential to limit risk

4. Vulnerability Statement

[Compile and list potential vulnerabilities applicable to the system assessed].

Vulnerability	Description
Brute Force Attack	The vulnerability to brute force attacks is prevelant when dealing with administrator access, and if this information were to be leaked we could see hacking of the websites on a massive scale. All information on the server would be at risk. To keep risk at a minimum, administrators are given complex passwords and told not to use the same password on multiple websites. There is little likelihood that this information could become public if each administrator follows the guidelines for password protection.
DDoS Attack	The inherent vulnerability to DDoS attacks is immeasurable. DDoS attacks have taken down many large company websites, and our website is still at risk until a CAPTCHA is placed somewhere on the website. DDoS attacks could potentially shut down the website and cause the TCP/IP handshake to fail resulting in no administrator or consumer access to the website.
SQL Injection	Similar to brute force attacks, on the Wordpress back-end we must assume that there is enough security to limit SQL injection attacks. The website does run on PHP, so it is able to be breached using SQL injection if these vulnerabilities are not fixed appropriately.
Unknown Vulnerability	There are many unknown variables that could lead to potential vulnerabilities, and thus it is important that both users and administrators use their best digital literacy and avoid any potential leaks via third-party websites, cookies, and phishing attacks.

5. Threat Statement

[Compile and list the potential threat-sources applicable to the system assessed].

Threat-Source	Threat Actions
Administrator Panel	If administrator panel is vulnerable to attacks, the entire website is in danger. To secure this area of the website, administrators must ensure that their passwords are kept secure and that they do not have their systems hacked by any means.
Customer Information Database	If the customer information database were to fall into the wrong hands, this could lead to many problems for both our company and the users. Identity theft, fraud, and other common financial crimes may be prevalent if we do not properly secure client information such as credit card numbers and shipping locations.

5. Risk Assessment Results

- The risk assessment has decided that the following four are the most important to be aware of when building the web-server and website. Keep in mind that the threats above can be kept to a minimum for best chance of security.

Item Number	Type	Data Being Stored	Impact	Likelihood	Organizational Value
1	Customer Info	Customer name, email, phone numbers, location, usernames, passwords, and identification numbers.	The impact of customer information being leaked is huge, as clients would no longer trust our services and would be more likely to go to third parties for their shopping necessities. Possible lawsuits can occur if this information were to be leaked.	Low	High — this is important customer information that cannot be leaked anywhere. The information must be kept secure under lock and key, possibly encrypted if placed on the cloud.

2	Employee Info	Employee names, usernames, and passwords	Employee logins for admin panels and e-commerce store editing are extremely important and the backbone of the entire service. If even one of these username /password combinations were to be leaked, it would be a disastrous set of events.	Medium	High — this is the second highest priority after payment information, I suppose it is at the same level of importance as payment information but the super administrator can disable access to any administrator account that may be inappropriately handling information so it is less of a total risk.
3	Payment Info	Credit card payment information and PayPal information	When processing payments through the e-commerce portal, client information must be kept securely encrypted through the internet and must be kept in a secure location, either on the cloud or locally for minimum security risks.	Low — dealt with all from the back-end of the website and if we're to add a SSL certificate to our website, the risks would be even lower.	High — loss of this information would be a disaster, and consumers would no longer trust our company if this information was leaked to third-parties. This is the highest priority.

4	Product Info	Critical figures to keep track of profits and deficits in regards to product sales	Low	Medium — might be leaked accidentally, since it is at the click of a button whether this information is kept private or public. Can be reversed easily.	Low — this information is all relatively meaningless for consumers, but helps the site runners actively understand the gross amount of product sales.