Computer Systems

Security Foundations

Week 1: Introduction to Information Security

Aidan Polivka

Feb 10, 2024

Table of Contents

Project Outline and Requirements (Week 1) 3

Organization Description 3

Proposed Migration Architecture 3

Project Requirements 4

Introduction to Information Security (Week 1) 5

The Need for Information Security 5

Why Ensure Compliance with Sarbanes-Oxley and PCI DSS? 5

Access Challenges for Consultants 5

Security Assessment (Week 2) 6

Access Controls and Security Mechanisms (Week 3) 7

Software and Database Security (Week 4) 8

Network Security (Week 5) 9

Project Outline and Requirements (Week 1)

Organization Description

Heartland Escapes is a chain of bookstores in Southeastern Nebraska. They started small with two stores in the capital city Lincoln, but due to successful social media marketing campaigns they have expanded to two other cities: Omaha, and Grand Island. These two new locations have continued to show success and deliver significant revenue. What sets Heartland Escapes apart from other bookstores is their use of events. They host several events throughout the year, including author meet & greets, scary story readings for kids on Halloween, fun Easter and Saint Patrick's Day parties, summer book reading for kids, etc. These events are well advertised and well attended because of Heartland Escapes social media presence. Because of Heartland Escapes quick growth, they've engaged in a modernization effort to migrate their technological infrastructure to an Azure hosted cloud environment. Their on-premises system was stood up in 2009 and hasn't received much of an upgrade over time, so they've contracted us as security experts to assess the security of their proposed migration effort.

Proposed Migration Architecture

The contractors working on the migrated architecture have a thorough document on how they plan to build this new infrastructure. They have taken security measures into account to the best of their ability, but it's our job to evaluate the planned infrastructure and provide more detailed suggestions as to how this infrastructure can achieve the desired level of security by Heartland Escapes.

"I suggest configuring Azure into two resource groups: one for data and infrastructure, and the other for applications. All resources should be in the us central region. In the application storage container, there will be three app services: one for the Point-of-Sale web application, one for the Inventory Service, and one for the public website. Azure App Services are like containers with a base operating system. In this case, I recommend running all services on a Windows system for simplicity. The app services would use the Premium v3 P1V3 hardware tier, which includes two vCPUs and 8 GB of RAM per instance, with the ability to scale up to 30 instances. In the data and infrastructure group, there would be an Azure SQL Server hosting both databases, and a virtual network (vNet) that manages firewall rules and security. A vNet Gateway would allow users to access the system via VPN. The public website would be the only part of the system outside of the vNet, accessible only through the gateway. The public website's IP address would also have access." (Polivka, 2023)

Later in the document, the author goes on to discuss the need for Azure Active Directory and role base security, which is an Azure component missing from this high-level proposal.

Project Requirements

Because their on-premises system was set up well before network and system security was standardized as a top priority, there are a lot of gaps in the security of their infrastructure. As they migrate into this new infrastructure, they want to prioritize security modernization as well. An important note is that Heartland Escapes transmits customer banking information for online transactions, so they must fall into compliance with the Payment Card Industry Data Security Standard (PCI DSS). They also would like to be able to store customer banking information in the future to set up an e-commerce website, which is even more reason to follow PCI DSS. For an additional twist, after the migration effort has taken place Heartland Escapes wants to go public and release a new IPO. So, not only do we need to ensure compliance with PCI DSS, but also the Sarbanes-Oxley Act regulations.

Our key goals in this security assessment are as follows:

- Evaluate requirements for the PCI DSS and Sarbanes-Oxley and ensure Heartland Escapes security policies meet these requirements.
- Evaluate the security risks of the proposed environment.
- Evaluate access control methods that are proposed, identify alternative controls, and provide our own proposal as security experts.
- Evaluate the need for controls to better protect data both at rest and in transit.
- Develop or redesign a secure network solution.

Introduction to Information Security (Week 1)

To perform what is required of us by Heartland Escapes, we must first review the proposed infrastructure and security model to ensure compliance with the Sarbanes-Oxley act and PCI DSS. We also need to know what risks are presented by remote hosting of the organization's system, the challenges that we as consultants will face for access, and the challenges that apply due to Heartland Escape's desire to take an IPO.

The Need for Information Security

The need for information security is clear. If Heartland Escapes wants to go public without risking fines for failing compliance, they need to secure user's information. That reason is strictly for the sake of Heartland Escapes, it's also a major risk to not secure user information for the sake of Heartland Escapes customers. If user data is leaked, a Heartland Escapes is sure to lose customers and reputation while hurting the consumers that keep their business running and the communities that built their business.

Why Ensure Compliance with Sarbanes-Oxley and PCI DSS?

PCI DSS is required guidelines for institutions interacting with customer banking information. Since Heartland Escapes transmits and will eventually store user banking data, they must comply with these guidelines or risk fines. Because Heartland Escapes plans to go public, they will be required to comply with regulations defined by the Sarbanes-Oxley act. Further discussion around the details of following these compliance regulations must be had.

Access Challenges for Consultants

Because Heartland Escapes' new environment is hosted in the cloud, we as consultants have no need to access on premises systems or to work on-site. This is beneficial to us so we can continue to work from home, or the home office. However, if they have sufficient access controls, we might run into roadblocks with permissions at the start of the audit process.

Security Assessment (Week 2)

TBD

Access Controls and Security Mechanisms (Week 3)

TBD

Software and Database Security (Week 4)

TBD

Network Security (Week 5)

TBD

References

Polivka, A. D. (2023). Modernizing “Heartland Escapes” to a Cloud-Hosted Infrastructure.