Computer Systems

Security Foundations

Week 4: Network Security

Aidan Polivka

March 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
Assets 6
Network Segregation 6
Risk Assessment Strategy 7
Risk Mitigation Options 7
Access Controls and Security Mechanisms (Week 3) 9
Access Controls of Existing Applications 9
Access Controls to the Wi-Fi Network 10
Network Authentication Schemes 10
Single Sign On 10
VPN Technologies 10
Software and Database Security (Week 4) 11
Regulatory Requirements of Sarbanes-Oxley 11
Regulatory Requirements for PCI DSS 11
Policies 12
Controls 12
Protecting Data 13
At Rest 14
In Transit 14
Network Security (Week 5) 15
Network Topography Breakdown 16
Access Controls Revisited 16
Intrusion Detection and Prevention 17
References 18

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)

Assets

As it stands, Heartland Escapes has several assets to protect. Thankfully, a lot of the work needed to identify these assets has already been completed by the teams working on the migration effort. They've already identified these assets from the on-premises machine because their goal is to segment them out into Azure controlled resources.

For data assets, Heartland Escapes has two databases: their accounting database and their inventory database. The data stored in the accounting database right now is strictly to track payments and charges for taxes. Eventually when they convert their system to an ecommerce website, they may end up storing customer account information. It's important that we consider this future goal when assessing the security around the database, because it'll be valuable information for the modernization effort. The inventory database is only for operations. Here they track the individual store's inventory, and this data is served to multiple applications for different purposes.

Heartland Escapes also has a few application assets, their public website, a home-grown point-of-sale system, and their inventory API. The only application that is accessible from outside the network is the public website, everything else is accessible by either the public website, or from within the network. All these applications are valuable and contain protected technology and code that should be safe guarded from prying eyes.

Network Segregation

Heartland escapes current system does not have any form of network segregation for their assets. This is generally a risk for multiple reasons:

Enlarged Attack Area. Without network segregation, all of Heartland Escapes assets are susceptible to a single attack on their server. It's the same principle of the adage, "putting all your eggs in one basket". You run the risk of something happening to that one basket, and all your eggs getting ruined at once. This is a precursor to what's called "lateral movement". If the bad actor has access to one service within your network, then they have easier access to elevate their own permissions, and access more critical parts of the network.

Data Integrity & Regulatory Compliance. It is typically poor practice to store highly sensitive data with insensitive data, specifically if they aren't expected to be used at the same time. Depending on the use case for said data, there may be standardized compliance guidelines around data storage that require network segmentation. This can be costly if not upheld.

Monitoring and Detection & Incident Response. Monitoring network traffic to a congested network hosting multiple business domains can be complicated. It is much simpler to monitor network traffic to a more modularized network ecosystem, which makes finding anomalies in such an

environment easier. As a result, if you're more able to monitor and detect network anomalies, then you'd be better able to respond to incidents. Having a tightly coupled network environment without any segregation of concerns can result in slow and complex incident responses.

Least Privilege Principle. The least privilege principle expects that only elements that need access to an asset, should have access to an asset. By having all resources on the same network, fundamentally this principle is broken, and causes a lot of risk.

Because our consulting firm's role on the project at this moment is strictly to analyze the proposed migration effort, we don't have any need to access the on-premises machine, or any of the hosted data or applications. Once the migration effort has taken flight with our assessment and suggestions in place, we can perform a secondary audit of their cloud hosted infrastructure from the comfort of our own homes, or the corporate office. If we did need to remote into the on-premises server, this would pose an additional risk to their system. Any additional holes we poke into their firewall, and any additional access points to their network can cause unnecessary risk.

Risk Assessment Strategy

Our game plan for analyzing Heartland Escapes ecosystem for risks is simple. We will analyze each service's vertical slice of functionality within the network. To elaborate, we'll take an individual service (starting with the inventory service since it is central to the rest of the system), and evaluate the service itself, it's positioning within the network, the database that the service is married to, and the network protocols used to communicate to internal and external structures. Once each service is evaluated, we'll look at the larger system and perform a high-level horizontal analysis of the network itself, and the data segregation.

Any found risk will have its own assessment. The most important structure to understand about each risk assessment is the risk level. We will use a 5 x 5 matrix to communicate the threat level of each risk. The x axis is 1-5 likelihood that this risk would be exploited, and the y axis is 1-5 risk severity. This heat map is a great way to determine what the threat level is and explain to Heartland Escapes the impact of the found risk. Here is a list of the expected contents of each assessment: risk scenario, identification date, existing security controls, current risk level, proposed treatment plan(s), progress status, residual risk (what is the risk level after each potential treatment), and the risk owner. (Cobb, 2024)

Risk Mitigation Options

As part of the risk assessment, a treatment plan must be chosen to propose to Heartland Escapes. What actions are taken to mitigate the risk at the end of the day is the decision of Heartland Escapes. If they want the expense of making code changes, or paying for third party services to mitigate risks, that is their prerogative. Our job is to offer *potential* resolution options. These resolution options can come in one of four different varieties, or a combination of any of these four varieties:

Avoidance. At this point, avoidance is an option we'll seldom suggest to Heartland Escapes, because their goal is to get our input on their modernization effort. However, this scenario is when the technology that poses the risk isn't valuable enough to fix. If it's deprecated, or unused, then the proposal could be for Heartland Escapes to discontinue use of the technology.

Transfer. This may be a commonly proposed option. Rather than suggesting code changes, we may propose that Heartland Escapes takes advantage of third-party software to mitigate an identified risk. For example, Azure (which happens to be the platform Heartland Escapes is migrating to) has tools for protecting against DDoS attacks. If it's found that Heartland Escapes' public website is susceptible to such attacks, it may be more worthwhile to suggest utilizing Azure's technologies over making code changes. Or we could prevent this attack from multiple angles by both *transferring* the mitigation effort and *reducing* the risk ourselves with code changes like rate-limiting requests.

Reduce. The third option is to reduce the risk by making explicit changes. Carrying forward the example of a DDoS attack, we could choose to *reduce* the ability of bad actors to perform such an attack by rate limiting requests from IP addresses to the public website. (Cobb, 2024)

Acceptance. The final option is to accept the risk. The only scenario in which we would ever suggest accepting a risk is if it's been determined that the risk threat is minuscule, and the cost to mitigate the risk through another means is more expensive than it's worth. Accepting a risk *is* a risk within itself and should be suggested with caution.

Access Controls and Security Mechanisms (Week 3)

In this section we're going to discuss some of the intricacies in the access controls of the modernized Heartland Escapes system. Because they're going to be cloud hosted rather than on site, each location is going to need to access the Point-of-Sale system via VPN. This shouldn't be new to most of the locations since that's functionality that has been in place for a while.

Additionally, instead of using the windows 2008 server active directory and manually creating accounts there, we'll be migrating to the Azure hosted Active Directory. Azure Active Directory will also manage this VPN access, which should be a quality-of-life upgrade for individuals interacting with the Point-of-Sale system and the inventory system. This should give more flexibility to the network administrators and ease of use.

Access Controls of Existing Applications

There are already role-based access controls in the originating system, thankfully, so we'll have a solid foundation to build upon in this migration effort. First let's look at the individual assets and the proposed access control mechanisms that will be used:

Who	**System**	**Access Control Mechanism**	
		Identification/Authentication	**Authorization**
Service	Accounting DB	Azure Managed Identity	RBAC
Individual	Accounting DB	Azure Active Directory	RBAC
Service	Inventory DB	Azure Managed Identity	RBAC
Individual	Inventory DB	Azure Active Directory	RBAC
Service	Inventory API	VPN + Azure AD/ SSO?	RBAC + OAuth 2.0 On-Behalf-Of
Service (public)	Inventory API	Azure Managed Identity	RBAC
Individual	Inventory API	VPN + Azure AD/ SSO?	RBAC + OAuth 2.0
Individual	Point-Of-Sale	VPN + Azure AD/ SSO?	RBAC + OAuth 2.0
Individual	Public Website	Public	N/A

As you can see, we're using role-based access controls for everything here. We'll have to define several roles, because not all individuals are going to need direct access to the databases. Not all individuals will need access to the point-of-sale system either. I'd like to bring attention to the Inventory API. Because the inventory API is supposed to be accessible by the public website, we need an Azure Managed Identity (cephalin, 2023) for the public website, and its own role to limit the set of functions it's able to perform on the Inventory API. Also, for communication to the Inventory API from other services, we'll use the Auth 2.0 On-Behalf-Of (jmostella) flow so that the individual performing actions/write operations to the inventory database can be audited.

Access Controls to the Wi-Fi Network

As stated previously, most applications will require network access via VPN. This will be managed using Azure Active Directory, and in most cases individuals who are listed in the active directory will have VPN access. The only systems that will not require VPN connection for access are the public website and the Inventory API. The only condition in which the Inventory API will be able to be accessed outside of the VPN is from the static IP address of the public website, and the built in Azure authentication from Azure Managed Identities.

Network Authentication Schemes

Single Sign On

According to GeeksForGeeks (2020), "Single Sign On (SSO) is an authentication scheme where users can securely authenticate and gain access to multiple applications and websites by only logging in with a single username and password". You can see instances of this all over the place, Google products are using this between Gmail, YouTube, and google drive, Microsoft uses this across all their products, and this technology is used in companies that have many applications. Heartland Escapes should aspire to be no different, and we're going to set them up in a way that if they continue to expand and build more in-house applications SSO implementation will be easy.

We're starting by implementing OAuth 2.0, which is a protocol used for authentication that is often used along side SSO. By signing into the application (point-of-sale as an example), using your Azure AD account, you'll receive an OAuth 2.0 JWT bearer token that will grant you access to other applications with the same identity provider. So, an individual could use the same bearer token they used to access the point-of-sale system for the inventory API. Because there is only one application that most individuals will use now, SSO is a little pointless. But the framework is there to build upon!

VPN Technologies

As stated previously, Heartland Escapes is no stranger to VPN technologies. They've been using a VPN for a while to communicate with the on-premises machine, and they'll be using a VPN here to tunnel into the virtual network that hosts the modernized system. In the modernized system, they'll be using the Azure VPN Gateway (cherylmc, 2024). This gateway will allow employees to operate in the Heartland Escapes system as if their machine were operating within the same network. This VPN requirement is just another added layer of security around Heartland Escapes resources and is a serious exterior layer of protection.

Software and Database Security (Week 4)

In our maintenance of software and database security, we need to build policies and controls that comply with the regulatory requirements of Sarbanes-Oxley (SOX) and they Payment Card Industry Data Security Standard (PCI DSS). As stated in previous segments, compliance with the requirements in critical for Heartland Escapes so they can effectively secure their customers' data and avoid fines.

Regulatory Requirements of Sarbanes-Oxley

There are many regulatory requirements within the Sarbanes-Oxley act. The subset of those requirements that impact information security can be boiled down into these regulations:

1. Section 404 – Management Assessment of Internal Controls. Heartland Escapes must be able to assess and report on the effectiveness of their internal controls over financial reporting. The effectiveness of information security controls also falls within this category.
2. Section 404(b) - Auditor's Attestation. Auditors of Heartland Escapes system must be able to attest to the effectiveness of Heartland Escapes security controls. Meaning the auditors will need access to the internals of Heartland Escapes system and be able to ensure that Heartland Escapes falls within data security and integrity compliance.
3. Section 409 - Real-Time Issuer Disclosures. Heartland Escapes must be able to communicate changes in the state of their financial condition securely and in real-time. This will require secure communication of financial information.
4. Section 802 - Criminal Penalties for Altering Documents. Any data tampering (internally or externally) can result in criminal penalties directed at Heartland Escapes. Production data must be highly secured, and a data retention plan should be in place that follows compliance guidelines.
5. Audit Committee Independence (Various Sections). The Audit committee must be a third party that is independent from Heartland Escapes. (Oxley, 2002)

Regulatory Requirements for PCI DSS

Within the System Modernization document (Polivka, 2023), there is a breakdown of the compliance requirements for PCI DSS. These are the tenants of maintaining compliance from a data security perspective:

1. Install and maintain a firewall system to protect cardholder data.
2. Avoid vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data on open, public networks.
5. Protect all systems against malware and update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy which addresses information security for all personnel.

Policies

In response to these regulatory requirements, we must build policies to ensure that Heartland Escapes maintains compliance with both the SOX act, and the PCI DSS. Here are five initial policies that should be implemented. This list is subject to expansion as the project continues, but for an initial assessment this should suffice.

Policy	**Description**
Data Encryption in Transit and at Rest	Data should be encrypted while it's being sent over the wire, and while it's dormant in Heartland Escapes databases
Real time auditing and log monitoring	To ensure data security, all activity to and from the Heartland Escapes should be monitored.
Least Privilege Data Access	Any access to data should be limited to individuals who need to see or transfer such data.
Regular Internal and External System Auditing	Heartland Escapes system should be audited internally and externally, looking for areas to improve and maintaining up to date with evolution in best practices.
Internal Training	Individuals working for or with Heartland Escapes should be subject to training programs for information security and suspicious behavior reporting.

Controls

The policies described are broad and wide sweeping. These are general policies to give Heartland Escapes pillars for SOX and PCI DSS compliance. However, these policies only answer the "what", and the "why", but neglect to show us "how" we maintain information security. In this section we will explain specific security controls around the policies outlined in the previous section.

Policy	**Control**
Data Encryption in Transit and at Rest	Any transmission of Heartland Escapes Data will be performed over secure network protocols (https, TLS, OpenVPN)
Data Encryption in Transit and at Rest	All data will be encrypted at rest
Data Encryption in Transit and at Rest	PII will be stored as encrypted text (SSN, Account Numbers, Dates of Birth, etc)

Real time auditing and log monitoring	PII and sensitive data will not be logged directly. (records will be identifiable by database primary keys)
Real time auditing and log monitoring	All logs (network, application, and database) will be monitored by secure and vetted software. Anomalies and suspicious behavior will be flagged as it's detected by monitoring software.
Real time auditing and log monitoring	An individual or group of individuals will be available 24/7 to respond to flagged suspicious behavior within network logs.
Least Privilege Data Access	Role Based Access Controls will be implemented to give individuals authorization to only the data and segments of the system they need to access
Least Privilege Data Access	No individual will have direct access to production SQL scripting or data
Least Privilege Data Access	Just-In-Time controls will be implemented so that data is only accessible when needed.
Least Privilege Data Access	Individuals performing data requests will need authentication using up to date authentication standards (currently OAuth 2.0)
Least Privilege Data Access	Passwords will be rotated every 3 months, the new password must differ from the past 12 passwords, and each password must be at least 16 characters, with at least 1 capital letter, 2 digits, and 2 special characters.
Regular Internal and External System Auditing	Internal information security specialists will stay up to date with changing system and data security standards. Our system will be audited by these individuals quarterly to ensure that we are within a tolerable threshold of security best practices.
Regular Internal and External System Auditing	SOX auditors will be granted access to systems and infrastructure during scheduled audits.
Regular Internal and External System Auditing	Regular internal vulnerability assessments will be conducted, and regular external penetration tests will be conducted. Regular phishing simulations will also be conducted.
Internal Training	Training will be conducted regularly and repeatedly over information security (phishing awareness, USB security, etc.)
Internal Training	"See something, say something" training will be implemented to ensure employees are holding each other accountable, and so they know that whistle blowers will be protected by the company.
Internal Training	Tailored training to security roles (RBAC) will be created and conducted. Individuals with elevated access and responsibilities should be trained accordingly.
Internal Training	Employee reporting procedures will be well defined, and easily accessible

Protecting Data

Data security and integrity are integral in maintaining SOX and PCI DSS compliance. Data must be secure both at rest and in transit. Data should only be directly mutable in lower-level environments (development and staging if applicable). Data should not be directly accessible or mutable in the production environment to ensure integrity and security.

At Rest

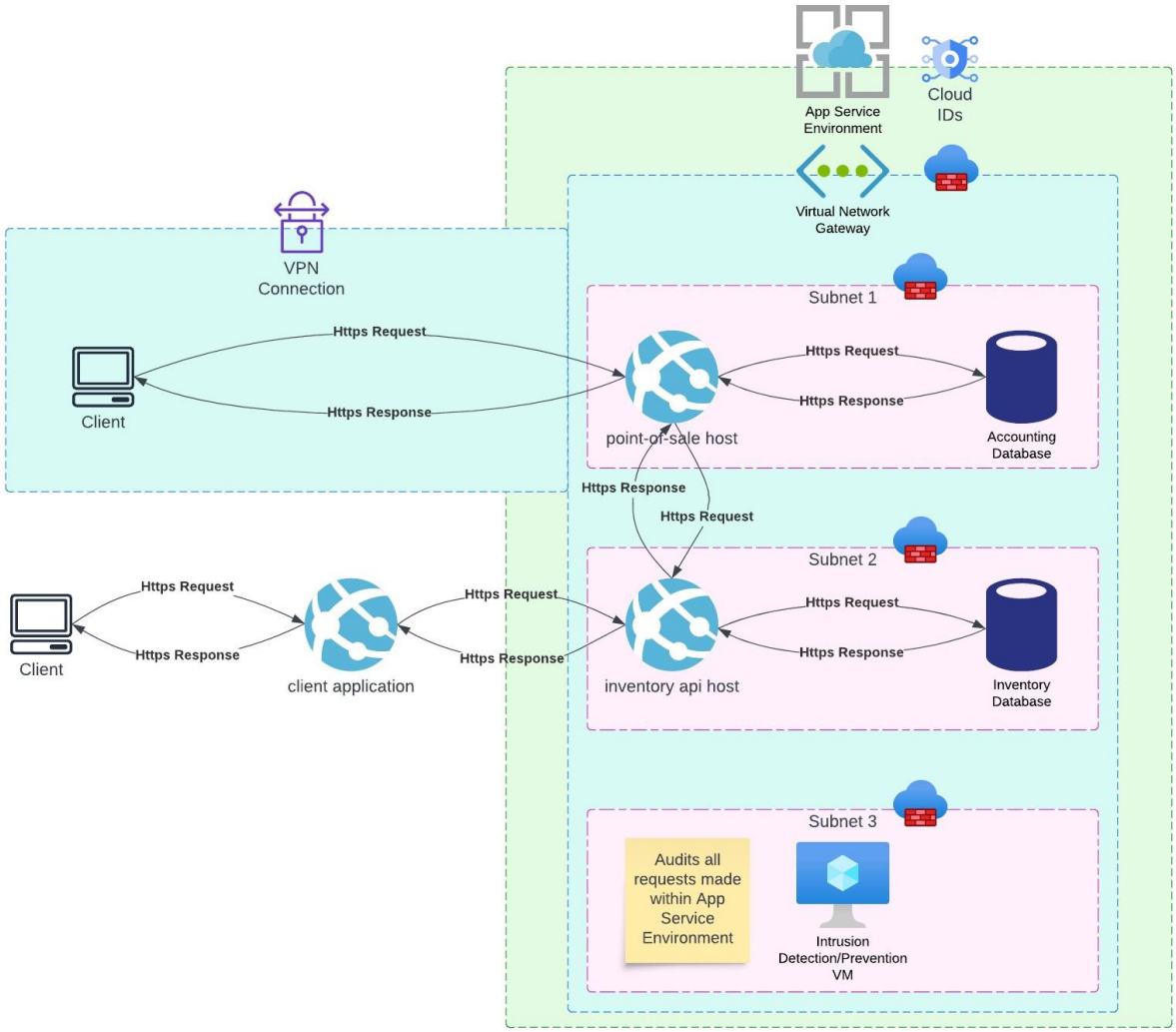
Azure SQL Databases offer encryption at rest, meaning that when data is not in use it is stored in an encrypted state. Additionally, PII (Personally Identifiable Information) should be stored in an encrypted state. SSNs and other PII should never be stored in clear text in the event that there is a data breach. This will ensure that bad actors who have gained access to the Heartland Escapes system are still unable to decrypt database records and steal customer information.

In Transit

Data in transit should also be encrypted using proper network protocols. Also, data should not be transferred unnecessarily over multiple network calls. In Heartland Escapes system, sensitive data access will be limited to a small number of service accounts, all utilizing https, TLS 1.3/SSL, and OpenVPN which are all standards in secure data transmission.

Network Security (Week 5)

Heartland Escapes network security maintenance is of utmost importance. This is where most external bad actors are going to try to infiltrate the system, and data in transit is going to be the most difficult data to secure. It's important that we also protect the accounting database and point of sale system from the public website. For the security structures in our network diagram, we'll take advantage of a VPN, an Azure App Service Environment, an Azure Virtual Network Gateway, and a subnet structure to segment our system and enforce specific firewall rules. Here is an expected network topography.



Network Topography Breakdown

The virtual network gateway will have its own firewall that only allows access from the public address of the public website. The subnets within the virtual network gateway will have their own firewalls that limit access of IP addresses from within the VNet gateway. Each subnet will need to have a rule in place for the VPN IP address range so the IT team can perform maintenance. All network traffic is limited to ports 443 and 22 in the production environment. For the development environment access will be extended to TCP connection on port 1433 & UDP on port 1434 for SQL Server development. This requires the use of the https protocol in any communication between services, ensuring encrypted messaging.

Virtual Network Firewall Configuration:

1. General
    a. Deny All
    b. Allow VPN IP address range on any IP address in VNet on port 443 (https) and 22 (ssh) (and TCP port 1433 & UDP port 1434 in dev)
    c. Allow Public Website public IP address range to Inventory API public IP address range on port 443
2. Subnet 1
    a. Deny All
    b. Allow VPN IP address range on any IP address in VNet on port 443 (and TCP port 1433 & UDP port 1434 in dev)
    c. Allow Inventory API public IP address range to Point-Of-Sale public IP address range on port 443
3. Subnet 2
    a. Deny All
    b. Allow VPN IP address range on any IP address in VNet on port 443 (and TCP port 1433 & UDP port 1434 in dev)
    c. Allow Public Website public IP address range to Inventory API public IP address range on port 443
4. Subnet 3
    a. Deny All
    b. Allow VPN IP address range on any IP address in subnet on port 22

Access Controls Revisited

Connections made to services within the VNet via VPN will be strictly controlled and audited. With the current network diagram, we don't see the additional role base access controls that further protect the system. Role based access controls will be in place to connect to the VPN, and these roles will further dictate access to virtual machines, services, and databases. Additionally, as stated in previous

sections, service accounts will use Azure Managed Identities to authenticate and authorize communication between them. This is not limited to the services within the VNet, the public website will also require this authentication and authorization mechanism to communicate to the Inventory API. All traffic to each service and database will be logged, and any SQL script ran will be logged (without data of course). All logging within the App Service Environment will be centrally accessible through the Azure Portal.

Intrusion Detection and Prevention

A significant part of the network topography that has yet to be mentioned is the Intrusion Detection and Prevention virtual machine. This is a Linux virtual machine with a tool called Suricata installed. Suricata is an intrusion detection and prevention system that monitors all network traffic. On a traditional network with virtual machines, simply setting up a Linux VM with Suricata within the virtual network would suffice. With the integration of Azure App Services, this may not be as trivial an exercise. We may need to route all traffic through the Suricata machine, further research needs to be done to better understand how we can integrate this IDPS tool into our network architecture.

Suricata offers a few types of intrusion detection. The primary form of detection is signature based, but it also offers anomaly-based intrusion detection. Meaning, it can understand the standard traffic seen in Heartland Escapes environment and flag behavior that is out of the norm. This could be incredibly important in DDoS detection. So, not only does it act as a wireless intrusion detection system, but a network behavior analysis system. (suricata.io)

Further, as an additional layer of security we'll build redundancy into our Intrusion Detection and Prevention. Azure offers a resource called Azure Firewall Premium, which allows for TLS inspection of outbound traffic, signature based IDPS, and URL filtering. The implementation of this IDPS should be simple compared to the Suricata implementation due to it being a native feature of the Azure Cloud Portal. This detection system will act primarily as a wireless intrusion detection system. (Horne, 2023)

Intrusion Detection and Prevention is highly important to our system. This allows us to meet the regulatory requirements in PCI DSS and SOX compliance for 24/7 monitoring of network traffic. This will significantly advance our ability to detect and resolve potential security issues at a super-human level. It also may catch threats that a firewall simply can't, like flagging malicious behavior of authenticated individuals. We can also configure our IDPS to automatically handle some types of suspicious behavior and notify security administrators for other types of suspicious behavior. This will take a lot of configuration and fine tuning to get our desired behavior. (redhat.com, 2023)

This is also a front-line effort at data loss prevention. If we can flag database scripts for large database update/delete/truncate transactions, then we can mitigate the need to restore from backups. Along similar lines, we can more easily audit select statements for large amounts of data, reducing the risk of individuals stealing and selling Heartland Escapes data.

References

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

Cobb, M. (2024, January 18). How to perform a cybersecurity risk assessment in 5 steps: TechTarget. TechTarget | Security. https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

cephalin. (2023, October 11). Tutorial: Access data with managed identity - Azure App Service. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cefcore%2Cdotnet

jmostella. (n.d.). Secure OAuth 2.0 On-Behalf-Of refresh tokens for web services - Azure Example Scenarios. Learn.microsoft.com. Retrieved February 26, 2024, from https://learn.microsoft.com/en-us/azure/architecture/example-scenario/secrets/secure-refresh-tokens

Introduction of Single Sign On (SSO). (2020, June 16). GeeksforGeeks. https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso/

cherylmc. (2024, January 4). About Azure VPN Gateway. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Oxley, M. G. (2002, July 30). Text - H.R.3763 - 107th Congress (2001-2002): Sarbanes-Oxley Act of 2002. Www.congress.gov. https://www.congress.gov/bill/107th-congress/house-bill/3763/text

Features. (n.d.). Suricata. https://suricata.io/features/

Horne, V. (2023, September 12). Azure Firewall Premium features. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/firewall/premium-features

What is an intrusion detection and prevention system (IDPS)? (2023, September 27). Www.redhat.com. https://www.redhat.com/en/topics/security/what-is-an-IDPS