Assessment Task 3

Cloud Native Apps and Security Automation

Yunseo Choi (14368117)

James Cook University Singapore

CP2422 Cloud and Data Centre Security

Mr. Steve Kerrison

8th August 2024

list of failures on dynamic test

1. Installation check
    - if word press is installed
2. Version check
    - WPSCAN_TOEKN is not set yet
3. HTTP check
    - HTTP 200: Serving on unencrypted HTTP
4. TLS version check
    - TLS version 13 not supported
5. TLS certificate check
    - Is default traefik certificate not used?
6. TLS prefer ecc
    - IS ecc key used rather than RSA?
7. Web Application Firewall checks
    - SQLi
        - No HTTP error on request with SQL injection

    - WAF: SQL injection defence?

- Path traversal

    - No HTTP error on request with path, got code 200

    - WAF: Path traversal defence?

Solutions

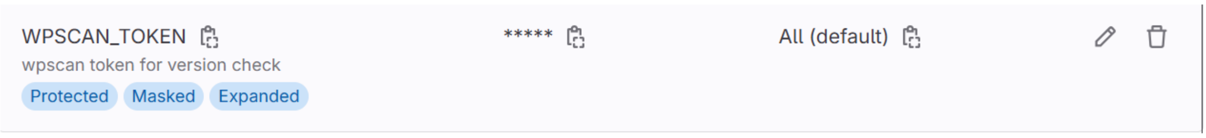
1. Installation check

No further research is required for this problem, as in the instruction, follow on installing word press, visit the deployment web URL enter user name and password to create word press website.

After changing port on web and websecure to 80, the wordpress installation error occurred again, I did change the service port to 80 and target port to 80, the error was addressed.

After solving another error in http check, this wordpress appeared to be not installed, it was addressed after redirection of http to https.

2. Version check



WPSCAN_TOKEN
wpscan token for version check
Protected Masked Expanded
*****
All (default)

added wpscan token first

I have encountered another problem after installing token which is 13 vulnerabilities with current wordpress version, thus I decided to change the version with less vulnerabilities first I tried 6.5.4 which gave me 3 vulnerabilities then next 6.2.2 but it gave 12 which is worse, as a result I have decided to use wordpress version 6.5.4 which is generating 3 vulnerabilities that is enough.

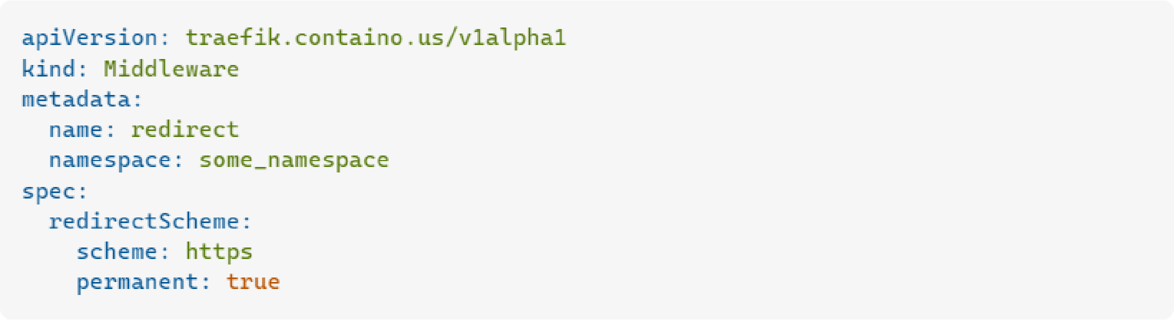
3. HTTP to HTTPS

for the task, I spent loads of time researching on solution to error, I have found middlewares, annotation and some more, however all of them did not work and brought me extra error message. Instead I tried changing the port number on web and websecure ingressroute to 80 on both, that was the time I was able to figure out solution.

After addressing another error in wordpress installation, error here occurred again.

This time with middlewares used, the error was solved.

but because it caused wordpress installation to show error, I did new attempt which is changing web secure port to 443, and wordpress deploy port to 443, it worked for http check, but it gave error in wordpress installation again. to address wordpress installation error, I had to redirect http to https using middlewares.



```
apiVersion: traefik.containo.us/v1alpha1
kind: Middleware
metadata:
  name: redirect
  namespace: some_namespace
spec:
  redirectScheme:
    scheme: https
    permanent: true
```

(Yuran, 2021)

after redirection, both http check and wordpress installation check passed security test.

4. TLS version check

without any research, by looking at error message and changing maximum tls to 13 which is version 1.3, I was able to solve the error

5. TLS certification check

I have looked into wordpress.yaml and tls-patch.yaml

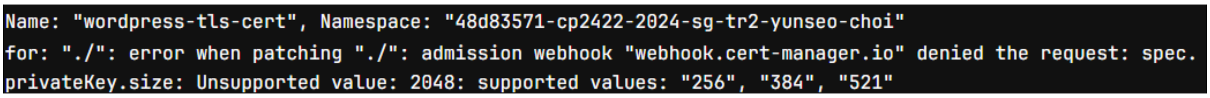
and I have foound out the domain name and match in wordpress.yaml is missing, and secret name of tls-patch.yaml is commented out. simply by filling in domain, match and uncommenting secret name, the error was solved.

before I go over the code, I did research on how to build certificate, then I went to readme.md and read one sentence small degree of change. After that I realized there is nothing to do with writing new code, so I started over and reached the solution.

6. TLS prefer ecc

   description of error says RSA is used rather than ECC, I went over files and found out that in wordpress.yaml, the key is set to RSA, so I changed it to ECDSA which is ECC and same as certificate.yaml

   after running the test, another error occurred which is

```
Name: "wordpress-tls-cert", Namespace: "48d83571-cp2422-2024-sg-tr2-yunseo-choi"
for: "./": error when patching "./": admission webhook "webhook.cert-manager.io" denied the request: spec.
privateKey.size: Unsupported value: 2048: supported values: "256", "384", "521"
```

   saying value 2048 is not supported, thus I changed value to 256, which is supported value.

7. Web application firewall check

   I was not able to apply waf structure in cluster management to my wordpress.yaml

   I do understand that waf filters HTTP traffic before it reaches your WordPress application. It uses Nginx with ModSecurity rules to detect and block malicious requests, ensuring that only legitimate traffic is forwarded to the application.

Task 2 Azure cloud

Compute Resources

Components:

- BCyber-GitLab
- BCyber-K3S
- bcyber-gitlab871
- bcyber-k3s290
- bcyber-azure-steve

bcyber-azure-steve is a component containing public key and SSH key type is RSA

- recommendation: Use ECC key type rather than RSA, because ECC is more efficient. ECC has shorter key length, thus time taken is shorter, which makes ECC more efficient.

BCyber-GitLab is a VM within resourc group of Bcyer.

It has several security and performance issues. The Azure Policy is not configured, leaving the VM vulnerable to misconfigurations. Microsoft Defender for Cloud monitors vulnerabilities, but the backup configuration shows an error, posing a risk of data loss. There are no disaster recovery measures, increasing the risk during region-wide outages. Auto-shutdown is not enabled, potentially leading to unnecessary costs if the VM is left running. Insights for logs and detailed monitoring are not enabled, limiting troubleshooting and performance monitoring. The VM uses standard security features but lacks advanced configurations

- recommendation: Implement Azure Policy, resolve the backup error, configure a disaster recovery solution, enable auto-shutdown policies, and enable Azure Monitor and Log Analytics.

BCyber-K3S is another VM, and is containing same problem with BCyber-Gitlab.

same recommendation is applied on BCyber-K3S.

BCyber-gitlab871 is a network interface connected to BCyber-Gitlab

BCyber-k3s290 is a network interface connted to Bcyber-K3S

both of them are network interface, providing internet connection to VM, thus segmenting virtual network into multiple subnet is required, and security audit on network interface is required.

Network segmentation is an architectural strategy that splits a network into several segments or subnets, with each one functioning as an individual small network (Palo Alto Networks, n.d.). Network segmentation provides network security personnel with a method to prevent unauthorized access and protect static IP addresses from both curious insiders and malicious attackers. This technique helps safeguard valuable assets, such as customers' personal information, corporate financial records, and highly confidential intellectual property, which are often considered the "crown jewels" of an enterprise (Palo Alto Networks, n.d.).

Regular network security audits are essential for identifying and proactively addressing vulnerabilities in the network infrastructure. By evaluating the firewalls, encryption protocols, and access controls, organizations can strengthen their defenses against potential threats. These audits also assess the effectiveness of current security measures and ensure compliance with industry regulations and best practices (Dig8ital, n.d.).

Storage Metrics

Components:

- BCyber-GitLab_OsDisk_1_822a8fe8d87e46ce85f3608b41eb64ba
- BCyber-K3S_OsDisk_1_54b34ba441dc41bb911fbe04ab6f6a16
- Data Disk IOPS Consumed Percentage (BCyber-GitLab & BCyber-K3S)
- OS Disk IOPS Consumed Percentage (BCyber-GitLab & BCyber-K3S)

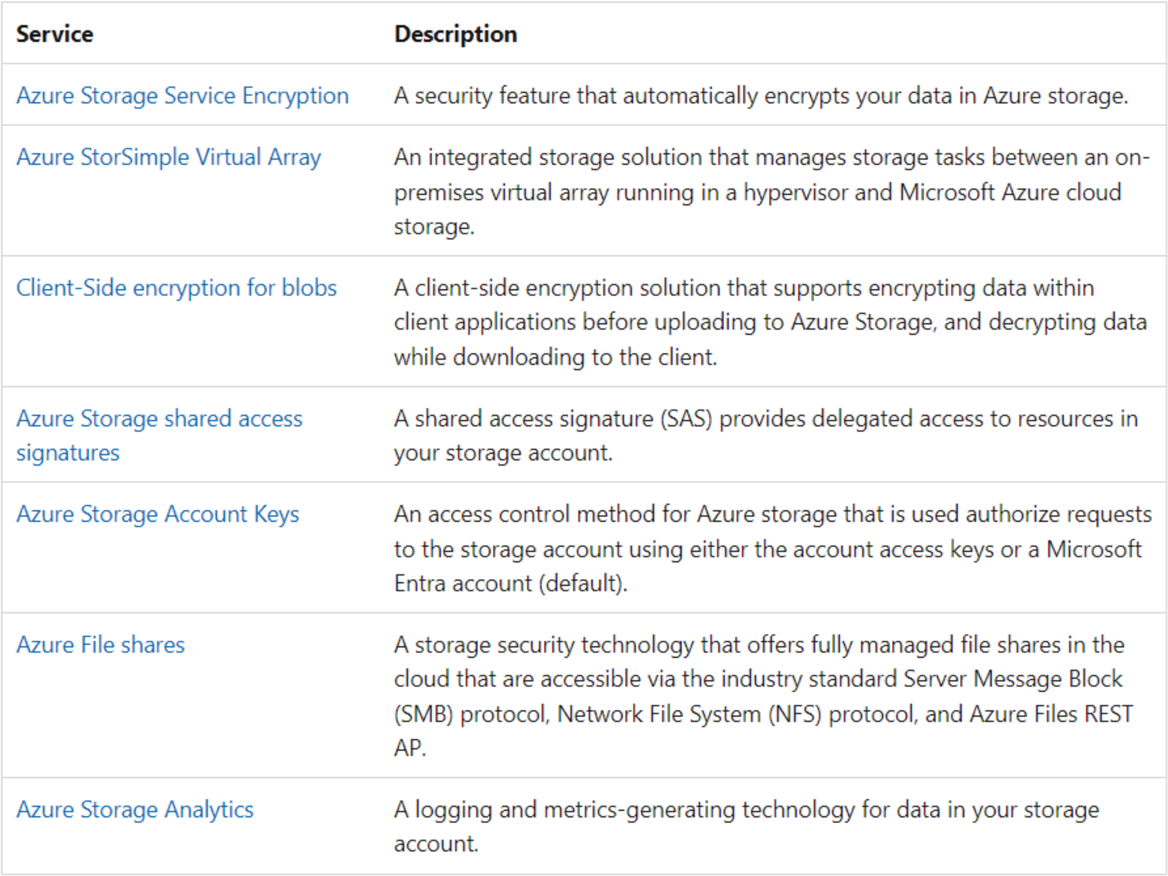
The BCyber-GitLab OS Disk is a 30 GiB Standard SSD LRS, offering a balance between cost and performance, with IOPS of 500 and throughput of 100 MBps, suitable for moderate I/O operations. The disk uses platform-managed keys for encryption, providing basic security. However, the VM is set with standard security settings, potentially lacking advanced features, and the current networking configuration (AllowAll) poses a security risk due to unrestricted network traffic. Regular monitoring and adjustments are necessary to maintain optimal performance and security.

The BCyber-K3S OS Disk has a size of 64 GiB and uses Standard SSD LRS storage, providing a balance between cost and performance. The disk has an IOPS of 500 and a throughput of 100 MBps, which are suitable for moderate I/O operations. The disk is encrypted using platform-managed keys, offering basic security. The VM is configured with standard security settings and the current networking configuration allows all traffic, posing a security risk due to unrestricted network access.

Data Disk IOPS Consumed Percentage BCyber-GitLab & BCyber-K3S and OS Disk IOPS Consumed Percentage BCyber-GitLab & BCyber-K3S is a property showing consumed percentage of two storages.

recommendation: Use customer managed key, enable advanced security features available in Azure services, enable Azure monitoring and log analytics to keep track of security events and disk performance, define a rule to limit access to certain data type, enable regular backup.

“Customer-managed keys in Azure Monitor give you greater flexibility to manage access controls to logs” (Microsoft, 2024).



Service	Description
Azure Storage Service Encryption	A security feature that automatically encrypts your data in Azure storage.
Azure StorSimple Virtual Array	An integrated storage solution that manages storage tasks between an on-premises virtual array running in a hypervisor and Microsoft Azure cloud storage.
Client-Side encryption for blobs	A client-side encryption solution that supports encrypting data within client applications before uploading to Azure Storage, and decrypting data while downloading to the client.
Azure Storage shared access signatures	A shared access signature (SAS) provides delegated access to resources in your storage account.
Azure Storage Account Keys	An access control method for Azure storage that is used authorize requests to the storage account using either the account access keys or a Microsoft Entra account (default).
Azure File shares	A storage security technology that offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol, Network File System (NFS) protocol, and Azure Files REST AP.
Azure Storage Analytics	A logging and metrics-generating technology for data in your storage account.

(Microsoft, 2024).

Above are services provided by Azure on storage security including log analytics.

For limiting access to certain data type, Azure services named role based access control is a solution, the description is “An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization” (Microsoft, 2024.).

Azure also has back up strategy there are Azure back up and Azure site recovery to prevent data loss. Azure back up backs up data and restore through Azure cloud (Microsoft, 2024.). Azure site recovery is replicaiting workload from primary site to secondary location for recovery purpose (Microsoft, 2024.).

Network Metrics

Components:

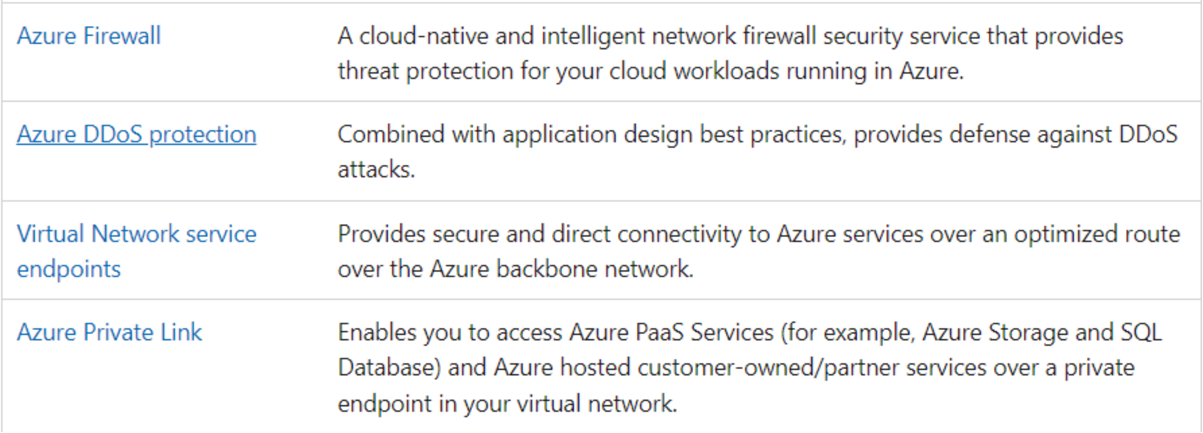
- Network In Total (BCyber-GitLab & BCyber-K3S)
- Network Out Total (BCyber-GitLab & BCyber-K3S)
- BCyber-GitLab-ip
- BCyber-K3S-ip

- BCyber-Net

The BCyber-GitLab public IP and BCyber-K3S-IP is statically assigned and properly provisioned, with a Standard SKU located in the Southeast Asia region. It is associated with the network interface bcyber-gitlab871, bcyber-k3s290 and the virtual machine BCyber-GitLab. However, no DNS name or domain name label is configured for the public IP. Additionally, DDoS protection is not enabled, which leaves the IP vulnerable to distributed denial-of-service attacks. These configurations and security gaps necessitate attention to enhance the overall security and manageability of the public IP address.

The BCyber-Net virtual network is located in Southeast Asia and uses the address space 10.188.0.0/16 with Azure-provided DNS services. Features such as DDoS protection, Azure Firewall, Private Endpoints, Peering are not configured. The absence of these features indicates potential security and connectivity gaps that could expose the network to various threats and inefficiencies.

recommendation: configure DDOS protection, firewall, private endpoints, vnet peering.



Azure Firewall	A cloud-native and intelligent network firewall security service that provides threat protection for your cloud workloads running in Azure.
Azure DDoS protection	Combined with application design best practices, provides defense against DDoS attacks.
Virtual Network service endpoints	Provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network.
Azure Private Link	Enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

(Microsoft, 2024.)

These are description of needed configuration.

Importance of each configuration:

Firewalls play a crucial role in network security by monitoring and filtering network traffic, preventing virus infiltration, blocking unauthorized access, upholding data privacy, and supporting regulatory compliance. Stateful inspection firewalls monitor active connections and ensure data packets meet security criteria, while next-generation firewalls offer advanced threat detection. Firewalls, working alongside antivirus software, identify and neutralize viruses before they breach systems. They also act as gatekeepers, preventing unauthorized access and ensuring only trusted sources can interact with the network. By scrutinizing data flow, firewalls maintain data privacy and protect sensitive information. Additionally, they enforce data protection standards and maintain activity logs, which are essential for regulatory compliance and audit trails, thus securing continued trust from stakeholders (Palo Alto Networks, n.d.).

DDoS protection ensures greater traffic capacity by blocking non-legitimate data packets, thereby optimizing network traffic and freeing up bandwidth for legitimate users. This results in an increased flow of legitimate concurrent accesses, allowing web services to handle a larger number of users, which is crucial for businesses that rely on the web for revenue. Additionally, DDoS protection supports scalability, enabling companies to build and maintain a scalable network infrastructure. It provides greater resource availability, allowing businesses to expand or reduce infrastructure performance as needed, ensuring continued growth and adaptability in the 21st century (UPX, 2023).

Using private endpoints for your storage account enables you to enhance security in multiple ways. Firstly, you can secure your storage account by configuring the storage firewall to block all connections on the public endpoint for the storage service. Secondly, it increases security for the virtual network (VNet) by allowing you to block data exfiltration from the VNet. Lastly, it enables secure connections to storage accounts from on-premises networks that connect to the VNet using VPN or ExpressRoutes with private-peering (Microsoft, 2023).

VNet peering simplifies the management of separate virtual networks in Azure by creating secure, direct connections between VNets, eliminating the need for public internet routes. This enhances security by keeping data within Microsoft's private network, improves performance through Microsoft's high-speed infrastructure, and supports scalability as the Azure environment grows. Additionally, it reduces costs by eliminating the need for a VPN Gateway, which is typically more expensive. VNet peering thus enables the construction of robust and secure network architectures in Azure (Kastwal, 2024).

Security Components

Components:

- BCyber-GitLab-nsg
- BCyber-K3S-nsg
- RecommendedAlertRules-AG-1

BCyber-Gitlab-nsg is

The BCyber-GitLab Network Security Group (NSG) has several inbound security rules, including allowing SSH (Port 22), HTTPS (Port 443), HTTP (Port 80), and a custom rule on Port 5050 for all sources and destinations. Additionally, it allows traffic from the virtual network and Azure Load Balancer while denying all other inbound traffic. The outbound rules allow traffic to the virtual network and the internet while denying all other outbound traffic. The NSG is associated with the BCyber-GitLab virtual machine and network interface. These rules are configured to allow necessary traffic but may require further restrictions to enhance security.

The BCyber-K3S Network Security Group (NSG) has several inbound security rules, including allowing SSH (Port 22) and custom web traffic on ports 80 and 443 for all sources and destinations. It also allows traffic from the virtual network and Azure Load Balancer while denying all other inbound traffic. Outbound rules permit traffic to the virtual network and the internet, while all other outbound traffic is denied. The NSG is associated with the BCyber-K3S virtual machine and network interface, indicating that the rules are designed to allow necessary traffic but may require further restrictions to enhance security.

RecommendedAlertRules-AG-1 is a Alert rules that are recommended for above 2 security group

recommendation:

Limit SSH (Port 22) Access: Restrict SSH access to specific IP addresses or IP ranges for both BCyber-GitLab and BCyber-K3S to minimize the risk of unauthorized access.

Use Web Application Firewall (WAF): Implement a WAF to inspect and filter HTTP/HTTPS traffic, adding an extra layer of protection against web-based attacks.

Review and Restrict Web Traffic: Ensure that the rules allowing traffic on ports 80 and 443 are necessary. If not, remove or limit access to specific trusted IP addresses or ranges.

Apply Network Security Best Practices: Regularly review and update NSG rules to follow the principle of least privilege. Ensure only necessary ports and protocols are open.

Enable alerts from RecommendedAlertRules-AG-1.

limiting access to files and folders can benefit in protecting sensitive information from unauthorized users and preventing data breaches. Its built-in user roles and data access controls ensure that only users with the correct permissions can access valuable data (Beckett, 2023).

A Web Application Firewall (WAF) protects web applications by filtering and monitoring HTTP traffic between the application and the internet. It defends against attacks such as cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection. As a layer 7 defense in the OSI model, a WAF is part of a broader suite of tools that together provide comprehensive protection against various attack vectors. Deploying a WAF places a shield between the web application and the internet, enhancing security (Cloudflare, n.d.).

Real-time IT alerts enable organizations to adopt a proactive stance against cyber threats, unlike traditional reactive cybersecurity approaches. By receiving instant alerts about suspicious activities, security teams can promptly investigate and implement preventive measures, helping to stay ahead of cyber adversaries (SendQuick, 2024).

Other Components

Components:

- bcyber.online
- bcyberdiagnostics

The bcyber.online DNS zone is managed within the BCyber resource group and is hosted in Azure with nameservers ns1-34.azure-dns.com, ns2-34.azure-dns.net, ns3-34.azure-dns.org, and ns4-34.azure-dns.info. With 10,000 record sets, the zone has extensive DNS configurations. Azure DNS provides domain hosting services using Microsoft's infrastructure, including tools for managing DNS records, retrieving record sets, and controlling access levels. The interface allows for setting up access controls to manage who can view or modify DNS settings, making it crucial to ensure that only authorized users have access to prevent unauthorized changes or potential security risks

The bcyberdiagnostics storage account is configured within the BCyber resource group, located in Southeast Asia, and uses StorageV2 with Locally Redundant Storage and a standard performance tier, currently in a succeeded provisioning state. The blob service has the hot access tier enabled, but features like account hierarchical namespace, blob versioning, and NFS v3 are not in use. Security settings require secure transfer for REST API operations, storage account key access is enabled, the minimum TLS version is set to 1.2, and infrastructure encryption is not in use. Networking settings allow public access for selected networks, no private endpoint connections are configured, network routing is managed by Microsoft, and access for trusted Microsoft services is enabled.

recommendation:

Enable Encryption

Maintain Documentation

Encryption can be enabled for an entire storage account or a specific encryption scope. When enabled, data is encrypted twice using two different algorithms and keys, once at the service level and once at the infrastructure level (Microsoft, 2024).

Cyber security documentation is crucial for understanding the importance of security governance, risk management, and compliance. It provides essential guidance, knowledge, and resources, serving as a reference manual for security professionals to consistently apply and uphold security measures across an organization (Newman, 2024).

General recommendation

without researching of possible recommendations and their importance, based on our 10 week lecture on cloud, my own recommendation on the current system is Implement Multi-Factor Authentication (MFA) for all users, use of automation to detect vulnerabilities, incident response on detected security issues.

For detection, SOAR (Security Orchestration, Automation, and Response) focuses on threat management, automating security operations, and responding to security incidents. It integrates additional data feeds, analysis, and automated functions based on identified incidents and threats. SOAR platforms enhance security by combining data gathering, case management, standardization, workflow, and analytics, enabling organizations to implement advanced defense-in-depth strategies.

Another strategy is usage of Azure sentinel serviced by Azure. According to (Microsoft, 2024.) Azure sentinel is "A scalable, cloud-native solution that delivers intelligent security analytics and threat intelligence across the enterprise"

MFA is essential strategy in identification and authorization. MFA is “A security provision that employs several different forms of authentication and verification before allowing access to secured information” (Microsoft, 2024.).

Terraform is one another strategy, Terraform enables the automation and management of infrastructure.

Lastly, Implement redundant system for continuous servicing despite of unexpected outages.

Further researches on why each security check is crucial

Proper installation of WordPress is critical for maintaining site security. According to WPBeginner, "A hacked WordPress website can cause serious damage to your business’s revenue and reputation" (WPBeginner, 2024). Ensuring that WordPress is correctly installed and configured significantly enhances the website's defense against potential threats

Vulnerabilities in WordPress sites pose significant risks, including unauthorized access and data breaches. Attackers exploit these weaknesses to gain control over websites, which can lead to unauthorized changes, data theft, or malicious activities (SiteLock, 2024). This compromises not only the integrity of the site but also its functionality and user trust. Addressing these vulnerabilities is crucial to maintaining a secure online presence, as it helps protect sensitive information, ensures the site's operational stability, and prevents potential legal and financial repercussions (SiteLock, 2024). Regular updates and vulnerability management are essential practices for safeguarding WordPress installations and preventing security breaches.

HTTPS is essential for securing web communications by ensuring that data transmitted between clients and servers is encrypted. The HTTP Strict Transport Security (HSTS) header is a key component in this process, enforcing the use of

HTTPS and helping to protect against downgrade attacks and cookie hijacking (Mozilla, 2024).

Strict Transport Security (HSTS) helps protect against man-in-the-middle attacks on public Wi-Fi networks. If you access a website using HTTPS and the site employs HSTS, your browser will enforce the use of HTTPS for future visits. This means that even if a hacker sets up a fake access point and tries to redirect you to a fraudulent site, your browser will automatically use HTTPS, preventing the hacker from intercepting and accessing your private data (Mozilla, 2024)

TLS 1.3 introduces several significant improvements over TLS 1.2, enhancing both security and performance. Firstly, TLS 1.3 offers enhanced security by removing outdated and less secure cryptographic algorithms, which reduces potential vulnerabilities. The protocol's simplification also minimizes the risk of implementation errors and security issues (A10 Networks, n.d.). In addition to security, TLS 1.3 improves performance by reducing the number of round trips required to establish a secure connection. This optimization speeds up the handshake process, leading to faster connection times and quicker load times for secure sites, thus enhancing the user experience (A10 Networks, n.d.). Another notable advancement is the enforcement of forward secrecy by default, which ensures that even if private keys are compromised, past communications remain secure—a significant improvement from TLS 1.2, where forward secrecy was optional (A10 Networks, n.d.). Additionally, TLS 1.3 reduces latency by optimizing the handshake process, making it particularly beneficial for applications that require low-latency communication (A10 Networks, n.d.). Overall, TLS 1.3 provides stronger security, better performance, and improved efficiency, establishing itself as the preferred choice for modern secure communications

Transport Layer Security (TLS) certificates, also known as Secure Sockets Layer (SSL) certificates, are crucial for securing online transactions and verifying domain identities. They encrypt data during transmission and authenticate the website’s identity, ensuring that users are interacting with legitimate sites. The TLS/SSL handshake, which occurs invisibly to users, establishes a secure connection between the web server and browser, indicated by HTTPS and a padlock icon in the address bar. This process protects user information and provides trust in the authenticity of the website (DigiCert, n.d.).

The main distinction between RSA and Elliptic Curve Cryptography (ECC) certificates lies in encryption strength. ECC offers equivalent encryption strength to RSA but with shorter key lengths,originally, as length of key is longer, the security lever is higher. however, ECC performs same level of security compared to RSA Adrian, 2023).

A web application firewall (WAF) enhances the security of web applications by filtering and monitoring HTTP traffic between the application and the internet. It defends against various attacks, including cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection, among others. By inspecting incoming traffic, a WAF can block malicious requests and protect the web application from potential vulnerabilities and exploits (Cloudflare, n.d.).

References

Adrian. (2023, September 8). RSA vs. ECC: A comprehensive performance analysis. Certauri. https://www.certauri.com/rsa-vs-ecc-a-comprehensive-performance-analysis/

A10 Networks. (n.d.). Key differences between TLS 1.2 and TLS 1.3. https://www.a10networks.com/glossary/key-differences-between-tls-1-2-and-tls-1-3/#:~:text=TLS%201.3%20offers%20

Beckett, S. (2023, January 25). Why limiting access to files is essential for security. GhostVolt. https://ghostvolt.com/blog/why-limiting-access-to-files-is-essential-for-security.html#:~:text=By%20limiting%20access%20to%20your,as%20hacking%20or%20phishing%20attacks

Cloudflare. (n.d.). Web application firewall (WAF). Cloudflare. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/#:~:text=A%20WAF%20or%20web%20application,and%20SQL%20injection%2C%20among%20others

Cloudflare. (n.d.). Web application firewall (WAF). Cloudflare. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

DigiCert. (n.d.). How TLS/SSL certificates work. https://www.digicert.com/how-tls-ssl-certificates-work#:~:text=TLS%2FSSL%20certificates%20are%20used,interacting%20with%20legitimate%20website%20owners

Dig8ital. (n.d.). Network security audits. Dig8ital.https://dig8ital.com/post/network-security-audits/#:~:text=Network%20Security%20Audits%20play%20a,infrastructure%20and%20address%20them%20proactively

Kastwal, S. (2024, May 21). Importance of VNet peering. K21Academy. https://k21academy.com/microsoft-azure/admin/azure-vnet-peering/#:~:text=Importance%20Of%20VNet%20Peering,-

Managing%20separate%20virtual&text=VNet%20peering%20brings%20several%20benefits,between%20resources%20in%20peered%20VNets

Microsoft. (2023, June 22). Private endpoints for Azure Storage. Microsoft Learn. https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

Microsoft. (2024, April 27). Storage security. Microsoft Learn.https://learn.microsoft.com/en-us/azure/security/fundamentals/services-technologies#storage-security

Microsoft. (2024, January 6). Customer-managed keys in Azure Monitor Logs. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal

Microsoft. (2024, June 6). Enable infrastructure encryption for your storage account. Microsoft Learn. https://learn.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable?tabs=portal

Mozilla. (2024, August 2). HTTP Strict Transport Security (HSTS). https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Newman, R. (2024, April 4). Why cyber security documentation matters. Medium. https://medium.com/@ricardonewman/cyber-security-documentation-67a7aad80bf4#:~:text=Cyber%20Security%20documents%20serve%20as,such%20as%20phishing%20and%20ransomware

Palo Alto Networks. (n.d.). What are the benefits of a firewall? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-are-the-benefits-of-a-firewall#:~:text=Firewalls%20operate%20as%20vigilant%20gatekeepers,access%20points%20within%20a%20network

Palo Alto Networks. (n.d.). What is network segmentation? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation#:~:text=Stronger%20network%20security,isolates%20attacks%20before%20they%20spread.

SendQuick. (2024, February 6). The crucial role of real-time IT alerts in cybersecurity. SendQuick. https://www.sendquick.com/the-crucial-role-of-real-time-it-alerts-in-cybersecurity/#:~:text=By%20receiving%20instantaneous%20alerts%20about,step%20ahead%20of%20cyber%20adversaries

SiteLock. (2024, April 1). How to fix WordPress vulnerabilities. https://www.sitelock.com/blog/how-to-fix-wordpress-vulnerabilities/

UPX. (2023, February 17). Benefits of DDoS protection. UPX. Retrieved August https://upx.com/en/post/benefits-of-ddos-protection/#:~:text=Ensuring%20greater%20traffic%20capacity,bandwidth%20is%20available%20for%20users

WPBeginner. (2024). The Ultimate WordPress Security Guide – Step by Step. Retrieved from https://www.wpbeginner.com/wordpress-security/

Yuran, A. (2021, July 29). K3s redirect HTTP to HTTPS. Stack Overflow. https://stackoverflow.com/questions/68575472/k3s-redirect-http-to-https