Cyber Security Threats to the Australian Education Sector:

Insights from PenetrationTesting

(2022-2024)


bersecurity
e Australia
catio
nsti
ur

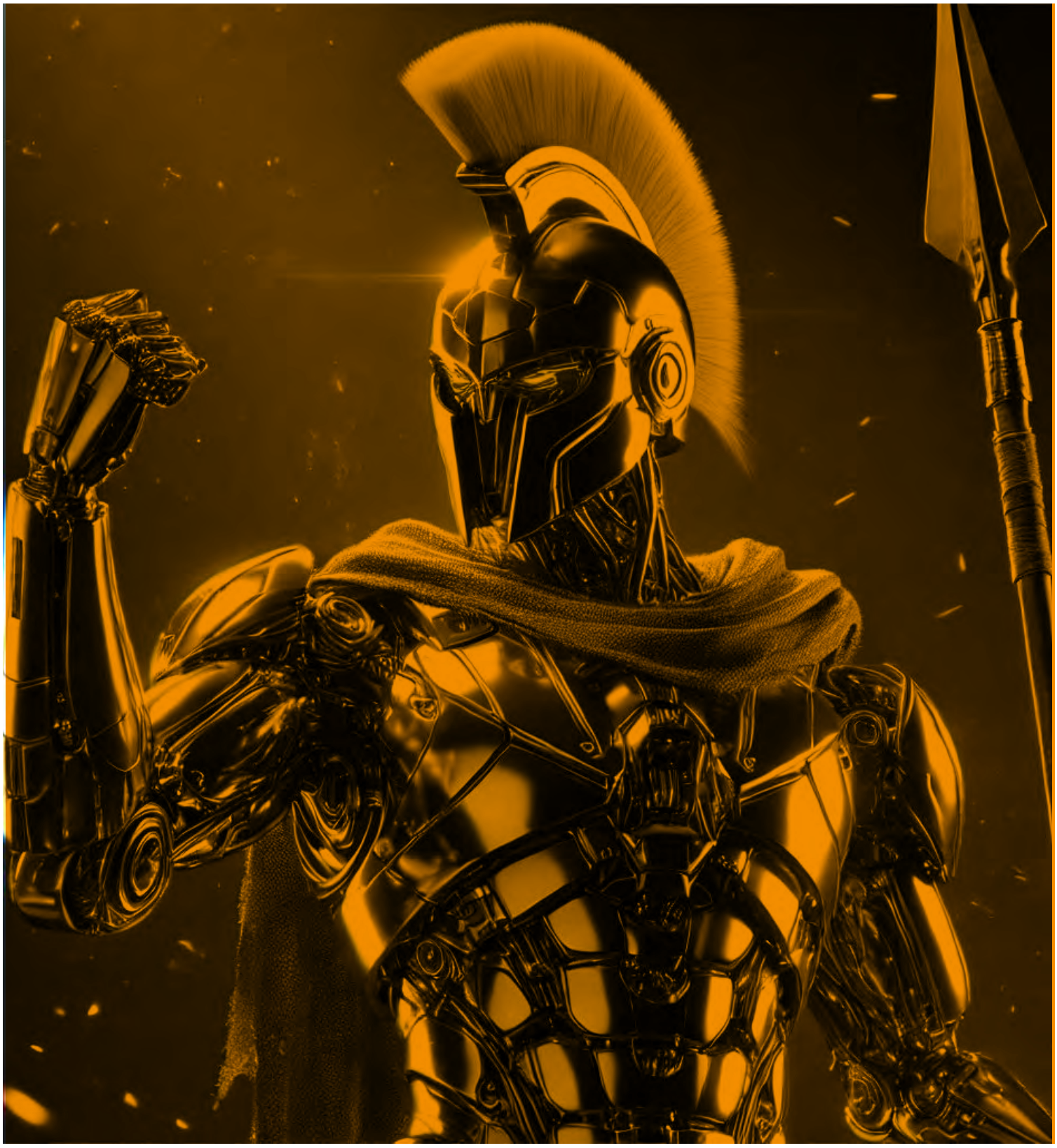
Executive Summary

The Australian education sector faces heightened vulnerability to cyber threats due to rapid digital transformation and widespread reliance on cloud services, learning management systems, and online resources. The data we collected from conducting numerous of internal, external and Cloud Penetration tests in schools between 2022 to 2024 uncovered common critical weaknesses in internal networks, external applications, and cloud infrastructures.

Schools manage highly sensitive data—such as personal, financial, and intellectual property—making them prime targets for cybercriminals. The increasing frequency and sophistication of attacks have led to significant financial losses, operational disruptions, and reputational damage. Data breaches in the sector have reached record costs, underlining the serious implications of these vulnerabilities.

This report provides an in-depth analysis of the current cybersecurity challenges in the Australian education sector, highlighting the most prevalent threats and detailing the specific vulnerabilities identified through testing.

Contents



SPARTANS SECURITY
YOUR CYBERSECURITY PARTNER

Spartans Security
P:+1300 20 90 23
E: info@SpartansSec.com
W: SpartansSec.com

Introduction Cybersecurity in Education

The digitisation of education has brought substantial benefits, from improving accessibility to fostering collaboration between educators and students. However, this digital transformation has also exposed educational institutions to a growing array of cyber threats. Globally, universities, schools, and research centres have been prime targets of cyberattacks, including ransomware, data breaches, and phishing. These attacks often exploit vulnerabilities inherent in outdated infrastructure, weak security practices, and the increasingly sophisticated tactics used by cyber adversaries.

In Australia, the reliance on cloud-based platforms, learning management systems (LMS), and digital tools has amplified these risks. Many institutions struggle to keep up with the security demands of the modern digital landscape. The growing volume of sensitive information handled by educational institutions—ranging from personal and financial data to intellectual property—makes the sector a prime target for cybercriminals. Furthermore, limited cybersecurity budgets and resources often lead to security gaps that adversaries can exploit.

Overview of Education Institutions

This white paper focuses on a number of schools and independent educational institutions in Melbourne. These institutions vary in size, from medium to large, and serve a diverse student population, mostly K- 12.

In addition to their academic focus, these institutions collectively manage a substantial array of digital assets to support their modern approach to education and communication. Their digital footprints include:

- **School Website**
- **Student Leaning Management Systems**
- **School Enterprise Resource Planning systems**
- **Parent and student Portals**

Moreover, many of these schools host subdomains dedicated to specific functions such as alumni networks, parent-teacher associations, and event management, showcasing their commitment to engaging their communities through digital channels. Learning management systems, such as Canvas or Schoolbox, are commonly used to facilitate remote or blended learning environments, providing secure access to coursework, assignments, and academic records.

These institutions also implement various cloud-based services, often using platforms like Microsoft 365 or Google Workspace for document management, email systems, and secure portals for faculty and administrative staff. Many schools have implemented security best practices, such as multi-factor authentication (MFA) and frequent updates to their digital platforms. However, despite their efforts, the ever-evolving cyber threat landscape continues to pose significant challenges

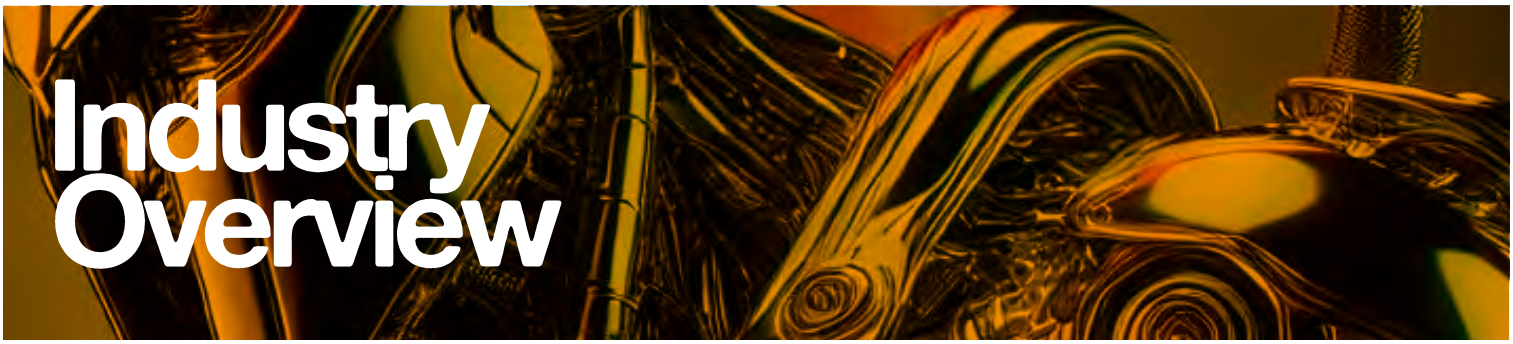
Objective

This white paper provides a comprehensive analysis of the cyber threat landscape affecting the Australian education sector from 2022 to 2024 by drawing on data collected from running internal and external penetration testing across these schools This paper highlights the common critical vulnerabilities within internal networks, external applications, and cloud infrastructures. These security gaps present significant risks to sensitive data and operational continuity, underscoring the urgent need for stronger cybersecurity measures.

The primary objectives of this white paper are to:

- Illuminate Prevalent Vulnerabilities: Identify and emphasize key security weaknesses uncovered during penetration testing conducted between 2022 and 2024 across Australian educational institutions.
- Analyse Threat Manifestations: Provide in-depth insights into how internal, external, and cloud-based threats leverage these vulnerabilities to compromise systems and data.
- Recommend Actionable Strategies: Suggest practical, actionable strategies to strengthen cybersecurity defences, with a focus on addressing areas of greatest risk.
- Promote a Proactive Security Approach: Advocate for the adoption of a layered, proactive cybersecurity strategy that aligns with broader industry trends, emphasizing the importance of continuous monitoring, regular updates, and comprehensive security policies.

This document aims to provide educational institutions with a clear roadmap to mitigate risks, protect sensitive data, and ensure operational resilience against the growing sophistication of cyber threats.



Industry Overview

The Australian education sector comprises universities, vocational institutions, schools, and other educational bodies. These institutions handle vast amounts of sensitive information, including student records, financial data, and intellectual property. In recent years, there has been a sharp rise in the number of reported data breaches in the education sector, driven by internal vulnerabilities, external threats, and a lack of advanced cybersecurity practices.

The Office of the Australian Information Commissioner (OAIC) and the Australian Cyber Security Centre (ACSC) have both noted significant cybersecurity incidents in the sector. Educational institutions, especially universities, must deal with increasingly sophisticated cyberattacks while managing legacy systems and strained cybersecurity budgets.

Findings: Vulnerabilities in the Australian Education Sector

The penetration tests conducted from 2022 to 2024 have uncovered significant vulnerabilities in the cybersecurity posture of educational institutions. These weaknesses span internal networks, external systems, and cloud infrastructures, exposing institutions to a range of cyber threats including data breaches, ransomware, and unauthorized access.

Internal Methodology

Initial User Enumeration:

The engagement begins with a reconnaissance phase, where Kerbrute is employed to identify valid users within the target environment. By leveraging the xato-net-10-million-usernames.txt list from SecLists, an extensive username enumeration is performed to detect legitimate users, marking the first step in understanding the target's Active Directory structure.

Password Spraying:

Once valid usernames are obtained, a password spraying technique is applied. In this phase, rather than launching a brute-force attack, the valid usernames themselves are used as passwords. This method minimizes detection risk, as it relies on legitimate login patterns while targeting low-hanging credentials.

Post-Access Enumeration:

With access gained through the identified credentials, further enumeration of the network is conducted. This involves querying key assets, particularly looking for weaknesses in Active Directory Certificate Services (ADCS), a common vulnerability in many environments.

Privilege Escalation via ADCS:

By exploiting the vulnerabilities within ADCS, the attacker escalates privileges within the Active Directory structure. This enables the acquisition of Domain Administrator (DA) credentials, allowing full control over the domain.

Domain Compromise:

With DA credentials in hand, the attacker uses the hashes to compromise the domain. The attacker now has full control over the domain and can move laterally, extract sensitive data, and persist in the environment undetected.

Weak Password Management

Summary

A significant number of users, including staff and students, are using weak and easily guessable passwords, such as school names combined with basic numeric sequences like “123,” or even using their username as the password. These practices significantly increase the risk of unauthorized access to systems and data. In addition, many organizations fail to enforce basic account lockout policies, leaving systems exposed to brute-force attacks. This lack of enforcement makes internal password spraying and brute-force attempts easier for attackers to carry out without being detected or stopped.

Details

- During internal audits, numerous examples of weak password practices were discovered. These include passwords like: 123456
- In several cases, passwords were found to be identical to the usernames, significantly increasing vulnerability.

Privileged Account Mismanagement

Several privileged accounts, including administrative users and service accounts, were found to use weak passwords. This is particularly concerning because privileged accounts have broader access to critical systems and sensitive data. If these accounts are compromised, the impact is far greater than with standard accounts.

- A lack of strict password complexity requirements for these privileged accounts was observed, making it easier for attackers to guess or crack them using simple techniques.

Internal Password Spraying Vulnerability

- Due to weak password policies and the absence of adequate account lockout mechanisms, the network is highly vulnerable to internal password spraying attacks. These attacks involve using a single, commonly used password across multiple user accounts, exploiting the lack of complexity in password choices.
- During penetration tests, it was demonstrated that password spraying with weak passwords yielded access to a large number of accounts within a short time, underscoring the need for stronger controls.

Number of Accounts with “Password Never Expires” Setting

- A concerning number of accounts were found to have the “Password never expires” flag enabled, which increases long-term risk. Accounts with this setting are particularly vulnerable to compromise because users are never forced to change their passwords, allowing weak or compromised passwords to remain in use indefinitely.
- Specifically, several administrative and service accounts were found with this setting, posing an even greater risk as they often have elevated privileges and persistent access to critical systems.

Recommendations

To address these issues, the following steps are recommended to strengthen password management and reduce vulnerabilities:

1. Enforce Strong Password Policies

- Require all users to adhere to strong password guidelines, including a minimum of 12 characters, and a mix of uppercase and lowercase letters, numbers, and symbols.

- Implement a password blacklist to prevent users from selecting common or easily guessable passwords like “Password123” or variations of the school’s name.

2. Implement Account Lockout Policies

- Introduce account lockout mechanisms to limit the number of failed login attempts. For instance, after five failed attempts, the account should be temporarily locked for a short duration or require administrator intervention to unlock.

- Monitor for failed login attempts and set alerts for unusual behaviour, such as a high number of attempts on multiple accounts.

3. Regularly Audit Privileged Accounts

- Conduct regular audits of privileged accounts to ensure strong password practices are enforced. Ensure that password complexity requirements are higher for accounts with administrative or elevated access.

- Consider implementing Privileged Access Management (PAM) solutions to enforce strict access controls for administrative accounts, requiring additional authentication or approval workflows for sensitive operations.

4. Mitigate Password Spraying Risks

- Implement Multi-Factor Authentication (MFA) for all user accounts, particularly for accounts with elevated privileges, to prevent attackers from gaining access using a password spraying attack.

- Educate users on the dangers of weak passwords and train them to recognize and respond to social engineering and phishing attacks, which often precede password-based attacks.

5. Address “Password Never Expires” Accounts

- Review all accounts with the “Password never expires” flag and enforce regular password changes for all accounts, especially those with privileged access.

- Where password expiration may not be feasible for service accounts, consider using Managed Service Accounts (MSAs) or Group Managed Service Accounts (gMSAs), which automatically handle password rotation securely.

By enforcing stronger password policies, implementing account lockout mechanisms, and regularly auditing privileged accounts, educational institutions can greatly reduce their exposure to brute-force attacks and password-based compromises.

Outdated SMB Protocols

Summary

Many schools continue to rely on outdated SMB (Server Message Block) protocols, such as SMBv1, which lacks modern security features and is highly vulnerable to exploitation. Additionally, critical security controls like SMB signing are often disabled, leaving systems susceptible to lateral movement attacks. Once an attacker gains initial access to a network, outdated SMB protocols allow them to move between systems with minimal resistance, escalating privileges and accessing sensitive resources.

Details

Usage of Legacy SMB Versions (e.g., SMBv1)

- Several network scans revealed that many institutions are still using SMBv1, a protocol known for its vulnerabilities and exploited in high-profile attacks like WannaCry. Despite its deprecated status and the availability of more secure versions (SMBv2/SMBv3), these older versions remain in use for legacy applications or file-sharing services.

- SMBv1 lacks essential security features, including encryption and stronger authentication mechanisms, making it easy for attackers to exploit and gain unauthorized access to shared resources.

Disabled SMB Signing

- SMB signing, which helps protect against man-in-the-middle attacks by ensuring the integrity of SMB communications, is often disabled in many environments. Without SMB signing, an attacker can intercept, modify, or replay SMB traffic, making it easier to compromise user credentials or inject malicious code.

- During penetration tests, it was found that environments without SMB signing were significantly more vulnerable to lateral movement. Attackers could easily pivot from one compromised system to another without raising alarms.

Lateral Movement Risk

- Outdated SMB protocols are a key enabler for lateral movement within compromised networks. Once an attacker gains a foothold, they can leverage insecure SMB connections to move laterally, map shared drives, steal credentials, and eventually escalate their access.

- The lack of modern SMB protections allows attackers to maintain persistence and access critical systems without detection, putting sensitive student, staff, and research data at risk.

Interoperability with Modern Security Solutions

- Systems relying on older SMB protocols are often incompatible with modern security solutions, such as network segmentation tools, encryption services, or threat detection platforms. This incompatibility makes it harder for institutions to implement comprehensive security measures across the entire network.

Recommendations

To address these risks and protect against lateral movement through outdated SMB protocols, the following steps are recommended:

1. Disable SMBv1 and Enforce Use of SMBv2/SMBv3

- Disable SMBv1 across all systems to mitigate vulnerabilities that are commonly exploited by attackers. Microsoft has deprecated SMBv1 due to its security risks, and institutions should migrate to SMBv2 or SMBv3, which offer improved performance and security.

- Conduct a full audit of systems and services that rely on SMBv1 and develop a migration plan to transition them to secure SMB versions.

2. Enable SMB Signing

- Enable SMB signing across all systems, particularly for sensitive file shares or systems that manage critical data. This ensures the integrity of SMB communications and reduces the risk of man-in-the-middle attacks.

- Enforce SMB signing policies for all administrative shares and network file-sharing servers, especially those connected to privileged accounts.

3. Limit Lateral Movement with Network Segmentation

- Implement network segmentation to isolate critical systems and reduce the ability for attackers to move laterally across the network. Use firewall rules and virtual local area networks (VLANs) to restrict unnecessary SMB communication between systems.

- Adopt zero trust principles that verify every connection request, preventing unauthorized lateral movement even if an attacker has infiltrated the network.

4. Apply Patches and Regular Updates

- Regularly apply patches and security updates to systems that use SMB protocols. Many vulnerabilities within SMBv1 have been patched over the years, and ensuring that systems are up-to-date helps reduce the attack surface.

- Ensure all devices are configured to auto-update, particularly for critical security patches related to SMB.

5. Monitor SMB Traffic and Anomalies

- Use Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) platforms to monitor SMB traffic for anomalies such as excessive file access or unexpected logins. This can help detect unauthorized lateral movement before major damage is done.

- Implement logging and alerting on SMB connections, focusing on unusual traffic patterns, unauthorized shares being accessed, or suspicious access attempts to critical systems.

By disabling outdated SMB protocols, enabling SMB signing, and applying stronger lateral movement controls, educational institutions can significantly reduce their exposure to attacks and protect sensitive data from being compromised by advanced threat actors.

Active Directory Certificate Services (ADCS) Misconfigurations

Summary

Misconfigurations in Active Directory Certificate Services (ADCS), particularly in commonly exploited protocols like ESC8 (Enterprise Subordinate CA misconfiguration) and ESC1 (misconfigured certificate templates), leave schools vulnerable to a range of attacks. These flaws can allow attackers to issue unauthorized certificates, enabling them to impersonate legitimate users or systems, potentially gaining unauthorized access to sensitive resources, and escalating privileges across the network. Properly securing ADCS is critical to maintaining the integrity of authentication and identity management systems.

Details

ESC8 (Enterprise Subordinate CA Misconfiguration)

- The ESC8 misconfiguration arises when an enterprise subordinate CA (Certification Authority) is improperly configured. This can allow unauthorized users or services to request certificates that are then used to impersonate trusted network identities.
- Attackers exploiting ESC8 can issue rogue certificates for privileged user accounts or even domain controllers, allowing them to impersonate these entities and gain high-level access within the network.
- During audits, several institutions were found to have ADCS servers where enterprise subordinate CAs were misconfigured, leaving them vulnerable to exploitation.

ESC1 (Misconfigured Certificate Templates)

- The ESC1 vulnerability involves misconfigured certificate templates that allow attackers to request certificates for accounts they control, even if those accounts should not have access to privileged certificates. These misconfigurations often involve template permissions not being restricted to the intended users or groups.
- Attackers exploiting this can obtain certificates with elevated privileges, effectively bypassing multi-factor authentication (MFA) and other security controls, and gaining persistence within the network.
- Institutions with poorly managed ADCS environments are at risk of attackers using ESC1 misconfigurations to escalate privileges and move laterally within the network.

Certificate Impersonation and Privilege Escalation

- Once attackers have unauthorized certificates, they can impersonate legitimate users, administrators, or even domain controllers. This allows them to authenticate to various systems and escalate privileges without detection.
- During penetration tests, several examples of unauthorized certificate issuance were observed, where attackers could gain high-level access and perform administrative tasks by exploiting improperly configured certificate templates.

Potential Network Takeover

- Misconfigured ADCS systems, especially in larger institutions, present a significant risk of complete network takeover. With rogue certificates, attackers can compromise sensitive resources, bypass authentication controls, and establish long-term persistence, compromising both user data and operational systems.

Recommendations

To mitigate the risks posed by misconfigurations in ADCS, the following steps are recommended:

1. Audit and Secure Certificate Templates

- Conduct a thorough audit of all certificate templates in the ADCS environment. Ensure that permissions are properly set, limiting certificate issuance to only authorized users and groups.
- Remove or restrict any legacy certificate templates that are no longer required, and verify that modern cryptographic standards are being used for key generation and encryption.
- Limit the scope of who can request certificates based on security groups, preventing unauthorized users from acquiring certificates with elevated privileges.

2. Enforce Strong CA Configuration

- Properly configure enterprise subordinate CAs to prevent unauthorized users from requesting certificates. Ensure that ESC8 misconfigurations are remediated by following Microsoft's best practices for securing CA hierarchies.
- Regularly review CA configurations to ensure that proper access controls are in place, especially for high-privilege certificates.

3.Implement Role-Based Access for ADCS Management

- Implement strict role-based access control (RBAC) for managing ADCS and certificate issuance. Only authorized administrators should have the ability to create or modify certificate templates, request high-privilege certificates, or manage CA infrastructure.
- Consider segregating ADCS management roles to reduce the risk of insider threats and limit the scope of potential attacks.

4. Monitor Certificate Issuance

- Enable logging for all certificate issuance activities and integrate these logs with a SIEM (Security Information and Event Management) system. This allows for continuous monitoring of who is requesting certificates and helps detect any unauthorized or suspicious certificate activity.
- Set up alerts for unusual or unexpected certificate requests, particularly for certificates associated with privileged accounts or key network infrastructure, like domain controllers.

5. Apply Patches and Security Updates

- Ensure that all ADCS servers and associated systems are fully patched and up to date. ADCS-related vulnerabilities are periodically discovered and patched by vendors, and keeping systems updated helps protect against known exploits.
- Apply specific hardening measures recommended by Microsoft and other security organizations to reduce the risk of certificate-based attacks.

6. Strengthen Authentication Mechanisms

- For high-privilege accounts, implement Multi-Factor Authentication (MFA), especially for certificate requests. This adds an extra layer of protection against rogue certificate issuance.
- Where possible, move to modern certificate authentication mechanisms, such as Public Key Infrastructure (PKI) certificates with strong cryptographic standards and enforce the use of hardware-based keys to secure sensitive certificates.

By addressing these ADCS misconfigurations and implementing the recommended security practices, educational institutions can significantly reduce the risk of attackers exploiting flaws in certificate services, preventing unauthorized access and ensuring the security of their network resources.

End-of-Life Operating Systems

Summary

We discovered that many schools continue to rely on unsupported or end-of-life (EOL) operating systems, such as Windows Server 2012, which no longer receive critical security updates or patches. This leaves systems highly vulnerable to widely known exploits and attack vectors. Attackers can easily compromise these outdated systems, leveraging known vulnerabilities to infiltrate networks, escalate privileges, and execute malicious activities without facing the security protections found in modern, supported operating systems.

Details

Use of Unsupported Operating Systems (e.g., Windows Server 2012)

- A significant number of servers and endpoints within educational institutions are still running Windows Server 2012 and other outdated operating systems. These systems have reached end-of-life, meaning they no longer receive security updates or patches from the vendor.
- Unsupported operating systems are especially attractive to attackers because the vulnerabilities they contain are well-documented and can be easily exploited using publicly available tools. The longer these systems remain in use, the greater the risk of a serious security breach.

Widely Known Vulnerabilities

- Many end-of-life operating systems are vulnerable to widely known exploits such as EternalBlue (used in the WannaCry ransomware attack), which can be easily weaponized by attackers. These vulnerabilities, once detected in a network, provide an easy entry point for unauthorized access.
- In one penetration test, several legacy systems running Windows Server 2012 were found to be unpatched against well-known exploits, exposing them to potential attack. Exploit attempts could be carried out with minimal resistance due to the lack of updated security measures on these platforms.

Network Exposure and Lateral Movement

- End-of-life operating systems significantly increase the risk of lateral movement within a network. Once an attacker compromises one outdated system, they can move laterally across the network to exploit other systems or access sensitive resources.
- Older systems often lack modern security features like Credential Guard, Secure Boot, and Windows Defender Application Control (WDAC), making it easier for attackers to maintain persistence and escalate their privileges within the environment.

Compliance and Regulatory Risks

- Continuing to run unsupported operating systems also introduces compliance issues, especially in sectors like education, which handle sensitive personal data. Regulatory bodies and data protection laws often mandate that systems must be kept up to date and secure, and the use of unsupported systems could result in financial penalties or loss of accreditation.

Operational Risks

- In addition to the security risks, outdated operating systems often lead to operational inefficiencies. Compatibility issues arise when legacy systems interact with modern applications or when attempts are made to integrate security solutions that are incompatible with older OS versions. This can result in service disruptions, delays, and increased maintenance costs.

Recommendations

To mitigate the risks posed by the use of end-of-life operating systems, institutions should take the following steps:

1.Prioritize Upgrades to Supported Operating Systems

- Immediately develop a roadmap for upgrading all end-of-life operating systems, such as Windows Server 2012, to supported versions like Windows Server 2022 or Windows 10/11 for workstations.

- Prioritize the upgrade of critical systems first, especially those that handle sensitive data or are part of essential infrastructure. Modern operating systems come with improved security features and continue to receive regular patches.

2.Apply Security Patches Where Possible

- For systems that cannot be immediately upgraded, apply any available patches or security hotfixes from the vendor. Some vendors may release critical patches for certain vulnerabilities even after the OS has reached end-of-life.

- Consider using Extended Security Updates (ESU) if upgrading is not feasible in the short term. ESU allows organizations to receive critical security patches for an additional fee for a limited time after the end-of-life period.

3.Isolate Legacy Systems

- If upgrading is not an immediate option, isolate legacy systems from the rest of the network. Use network segmentation techniques such as VLANs or firewalls to limit the exposure of these systems, reducing the likelihood of lateral movement in case of compromise.

- Disable unnecessary services and ports on these systems to reduce the attack surface. For instance, services like SMBv1 should be disabled if not required.

4.Strengthen Monitoring and Detection

- Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for attempts to exploit vulnerabilities in end-of-life systems. Deploy Security Information and Event Management (SIEM) solutions to monitor these systems closely for signs of compromise.

- Set up alerts for any unusual activity originating from or targeting these legacy systems, such as unexpected access attempts or lateral movement patterns.

5.Deploy Compensating Controls

- Where upgrades are delayed, implement compensating controls to mitigate the risks. These include enforcing Multi-Factor Authentication (MFA), restricting administrative access, and using application whitelisting to limit what can run on the legacy systems.

- Regularly audit legacy systems and conduct penetration testing to identify additional weaknesses and improve the overall security posture of the network.

6.Develop a Legacy System Decommissioning Plan

- Institutions should develop a clear plan to decommission legacy systems that cannot be upgraded. Transition critical services and data from end-of-life systems to supported platforms over time, ensuring that old systems are fully removed from the network.

- Evaluate whether the functions of legacy systems can be replicated or moved to modern environments like cloud services or virtualized systems, which offer better security and scalability.

By upgrading or isolating end-of-life operating systems and applying strong compensating controls, educational institutions can significantly reduce the security risks associated with outdated platforms and better protect their networks from exploitation.

LDAP Signing Not Enforced

Summary

Many have not enforced LDAP (Lightweight Directory Access Protocol) signing, a critical security feature designed to protect the integrity and confidentiality of communications between directory clients and servers. Without LDAP signing, communications between these systems are vulnerable to man-in-the-middle (MitM) attacks, allowing attackers to intercept, manipulate, and inject malicious traffic into directory queries and responses. This leaves sensitive user data and directory information exposed to unauthorized access and exploitation.

Details

Lack of LDAP Signing

LDAP signing ensures the authenticity of communications between Active Directory (AD) clients and domain controllers by adding digital signatures to the data. This prevents attackers from modifying or spoofing LDAP traffic.

In numerous schools, LDAP signing is not enforced, which means that clients and servers communicate in plain text, leaving the traffic vulnerable to interception and manipulation. Attackers with network access can exploit this weakness to intercept sensitive information or modify LDAP queries and responses.

Risk of Man-in-the-Middle Attacks

Without LDAP signing, attackers can perform man-in-the-middle (MitM) attacks by intercepting directory traffic. They can modify requests or responses to escalate privileges, gain unauthorized access to resources, or retrieve sensitive information like usernames, group memberships, and other directory attributes.

During security assessments, several educational institutions were found to have unprotected LDAP communications, which could be easily exploited to perform LDAP relay attacks, where the attacker forwards intercepted traffic to access systems as a trusted entity.

Exposed User Credentials and Directory Data

Unprotected LDAP traffic often contains sensitive information such as user credentials, group memberships, and access control details. By intercepting these communications, attackers can gather intelligence about the organization's users and systems, which could later be used for targeted attacks or lateral movement.

Penetration tests have demonstrated that attackers can retrieve password hashes, which can then be cracked offline, providing them with the ability to log into other systems with stolen credentials.

Vulnerability to Directory Manipulation

LDAP signing prevents attackers from modifying LDAP responses. Without this protection, attackers can alter directory information, for example, by changing group memberships or directory attributes to escalate privileges or gain access to restricted resources.

Inconsistent Adoption Across Systems

Some systems and applications within institutions may rely on LDAP for authentication or directory queries but are not compatible with modern LDAP security measures like signing. This results in inconsistent adoption of security controls, further increasing the risk.

During audits, it was found that while some modern applications support LDAP signing and secure LDAP (LDAPS), legacy systems still rely on plaintext LDAP communication, weakening the overall security posture of the institution.

Recommendations

To mitigate the risks associated with not enforcing LDAP signing, the following steps should be implemented:

1.Enforce LDAP Signing on All Directory Communications

- Enforce LDAP signing for all directory communications between clients and domain controllers. This can be done by configuring Group Policy to require LDAP signing:
- Set Domain controller: LDAP server signing requirements to Require signing in Group Policy to ensure that only signed LDAP requests are processed.
- For clients, set Network security: LDAP client signing requirements to Require signing to ensure all requests are signed. Ensure that both servers and clients are configured to support LDAP signing, reducing the risk of traffic being intercepted or tampered with.

2.Transition to LDAPS (Secure LDAP)

- Where possible, transition to using LDAPS (LDAP over SSL), which encrypts LDAP traffic, adding an extra layer of security by ensuring that all communications are both encrypted and authenticated.
- Update and configure domain controllers and LDAP clients to support LDAPS by obtaining and configuring SSL certificates for directory servers.

3.Identify and Upgrade Legacy Systems

- Conduct an audit of all systems and applications that rely on LDAP communication. Identify legacy systems that do not support LDAP signing or LDAPS and create a plan to upgrade or replace them with modern systems that support secure LDAP communication.
- For legacy systems that cannot be replaced immediately, isolate them through network segmentation and limit their access to only the necessary resources, reducing the impact if they are compromised.

4.Implement Network Monitoring for LDAP Traffic

- Use network monitoring and intrusion detection systems (IDS) to monitor LDAP traffic for signs of unusual activity, such as unauthorized queries or attempts to modify directory data.
- Set up alerts for any attempts to send unsigned LDAP requests to domain controllers, enabling swift detection and response to potential attacks.

5.Strengthen Logging and Audit LDAP Activity

- Enable logging for LDAP access and audit changes to directory objects to detect unauthorized access or modifications. Review logs regularly to identify suspicious activity, especially around user accounts, group memberships, and access controls.
- Ensure that audit logs are properly secured and sent to a centralized Security Information and Event Management (SIEM) platform for real-time analysis and alerting.

6.Regularly Test for LDAP Vulnerabilities

- Conduct regular penetration tests and security audits to identify any misconfigurations in LDAP settings or gaps in the enforcement of signing and encryption. Test for vulnerabilities such as LDAP relay attacks, MitM, and directory manipulation attempts.
- Continually assess the effectiveness of LDAP signing policies and ensure they are applied consistently across the entire network, covering all client-server communications.

By enforcing LDAP signing and transitioning to secure LDAP protocols, institutions can greatly reduce the risk of man-in-the-middle attacks, unauthorized directory access, and directory manipulation. These steps ensure the integrity of directory communications and protect sensitive user and organizational data.

Inefficient SOC Security Monitoring with 3rd Party SOC Services

Summary

It was quite common to find schools rely on third-party Security Operations Centre (SOC) services to handle their security monitoring and incident response. However, the inefficiencies in these outsourced services—such as poor integration with internal systems, delayed responses, and limited customization—leave significant security gaps. These inefficiencies can result in slow detection of threats, incomplete monitoring coverage, and suboptimal incident resolution, which can increase the likelihood of successful attacks going unnoticed. The reliance on external SOC providers without proper alignment to the institution's unique needs can lead to misaligned priorities and insufficient protection.

Details

1.Limited Integration with Internal Systems

Third-party SOC providers often struggle to integrate deeply with an institution's specific systems, such as learning management platforms, cloud services, or proprietary applications. This results in gaps in visibility and monitoring blind spots, where critical infrastructure may not be fully covered by the provider's standard toolset.

2.Delayed Incident Response

Third-party SOCs are often shared across multiple clients, leading to resource contention and delayed responses to incidents. These SOCs may operate under a "tiered" support structure, meaning lower-level analysts handle initial alerts before escalating more serious incidents to experienced personnel, adding delays to critical responses.

3.Lack of Customization and Contextual Awareness

Third-party SOCs often provide "cookie-cutter" services that do not account for the unique requirements of each institution. For example, the SOC might not be aware of the criticality of specific research data, the importance of specific faculty accounts, or the need for specialized monitoring around periods like admissions or exam seasons.

Educational institutions often have varying regulatory requirements and risk tolerance levels, but third-party SOCs may not have the flexibility to adjust their monitoring and incident response workflows to align with these needs. This lack of customization can result in critical events being mishandled or deprioritized.

4. Over-Reliance on Generic Detection Rules

Many third-party SOCs rely heavily on generic detection rules and pre-built alert configurations that might not be optimized for the education sector. As a result, the SOC may fail to detect sector-specific threats, such as intellectual property theft targeting research data or insider threats from compromised student accounts.

5. Limited Visibility into 3rd Party SOC Operations

Institutions often lack full transparency into how third-party SOCs operate, making it difficult to assess whether the SOC is meeting its contractual obligations or performing effectively. Institutions may receive monthly reports or dashboards, but the level of detail can vary, making it challenging to measure the quality and speed of incident detection and response.

Additionally, some SOC providers do not offer real-time access to logs or security data, limiting the institution's ability to perform its own independent analysis or respond in parallel with the SOC team.

Recommendations

To address the inefficiencies of third-party SOC services, institutions should take the following steps:

1.Ensure Deep Integration with Internal Systems

Work closely with the SOC provider to ensure full integration of critical systems, including learning management systems, cloud platforms, and sensitive databases. Provide the SOC with comprehensive documentation and access to internal IT resources to ensure the environment is properly monitored.

Conduct regular assessments to identify any gaps in monitoring coverage and ensure that all critical data sources, such as network traffic, endpoint logs, and cloud services, are being captured and analysed.

2.Negotiate Custom SLAs Tailored to the Institution's Needs

Review and negotiate service level agreements (SLAs) to ensure they are tailored to the institution's specific security requirements. SLAs should cover not just response times but also proactive threat hunting, dwell time reduction, and escalation procedures for critical incidents.

Ensure that the SOC is able to provide 24/7 monitoring or, if necessary, supplement third-party services with in-house staff or a second-tier provider during critical periods such as weekends and holidays.

3.Enhance SOC Customization and Contextual Awareness

Push for a higher level of customization from the SOC provider, ensuring that their monitoring configurations and response workflows are aligned with the institution's specific needs. For example, higher sensitivity should be applied to research databases or faculty accounts, while tailored alerts should be created for sector-specific threats.

Regularly review detection rules and collaborate with the SOC to fine-tune them based on the institution's evolving threat landscape. Ensure the SOC understands the institution's key assets, such as intellectual property, student data, and critical applications.

4.Deploy Hybrid SOC Models for Greater Control

Consider adopting a hybrid SOC model, where the institution maintains some internal monitoring capabilities alongside the third-party provider. This allows the internal team to monitor high-priority systems while outsourcing routine tasks to the third-party SOC, ensuring faster response times for critical incidents.

Use a hybrid model to also retain control over sensitive data and maintain real-time visibility into security events. This allows the institution to respond in parallel with the SOC in case of a major incident.

5.Invest in Regular Audits and Performance Reviews

Perform regular audits of the SOC provider's performance, including response times, false positive rates, and incident resolution effectiveness. Review their monthly or quarterly reports in detail and request more granular data if necessary.

Use external penetration testing or red teaming exercises to evaluate the SOC's ability to detect and respond to real-world attacks. Ensure that the SOC provider is able to rapidly detect and mitigate advanced persistent threats (APTs) and other sophisticated attacks targeting educational institutions.

6.Improve Communication Channels and Incident Transparency

Establish clear communication channels with the third-party SOC, ensuring that the institution has real-time visibility into ongoing incidents. Ensure the SOC provides detailed context around alerts and incidents, allowing the internal team to make informed decisions and take additional actions if needed.

By improving integration, customizing monitoring, and enhancing transparency and response times with third-party SOC services, educational institutions can significantly reduce the inefficiencies in outsourced security monitoring. This will enable faster detection and response to incidents, ensuring that the institution's critical assets are better protected from evolving threats.

External Vulnerabilities

Schools often face challenges in securing their internal systems, largely due to outdated protocols and weak security practices. Across all the schools tested we have found the following commonalities:

External Methodology

An external penetration test starts with reconnaissance and information gathering, where the we maps out the target's external network footprint. Assetfinder, amass, DNS enumeration, and Nmap are used to identify open ports, services, and public-facing systems such as web servers, email servers, and VPNs. Additionally, passive reconnaissance might involve scanning for subdomains, analyzing SSL certificates, and gathering publicly available information from sites like Shodan or Censys.

In the vulnerability discovery and exploitation phase, we identify weaknesses in the external infrastructur, looking for common attack vectors like outdated software, misconfigurations in web applications, weak authentication mechanisms, or exposed APIs.

Vulnerability scanners such as Nessus or OpenVAS help identify known issues, while manual testing is often used to explore business logic flaws or to chain vulnerabilities together for deeper access. Exploitation could range from SQL injection in web apps to exploiting weak credentials in exposed services.

The post-exploitation and reporting phase assesses the impact of successful attacks, such as data exfiltration, further network enumeration, and identifying ways to persist in the environment.

At this stage, we will document the entire process, including vulnerabilities found, attack paths, and sensitive data accessed.

Weak Password Management in External Systems

Summary

Many educational institutions have external portals and web applications that are vulnerable due to weak password management practices. Just like internal systems, these external-facing systems often suffer from poor password policies that allow users to set weak, easily guessable passwords. These vulnerabilities significantly increase the risk of brute-force attacks, where attackers use automated tools to try various combinations of usernames and passwords until they gain unauthorized access. Without robust password policies and protections in place, these external systems remain an easy target for attackers looking to exploit weak credentials.

Details

Weak Password Policies on External Applications

External systems, including student and staff portals, learning management systems (LMS), and web applications, often allow users to set weak passwords such as “password123,” or “University2023.” Many systems do not enforce password complexity requirements like a minimum length, use of special characters, or the inclusion of both uppercase and lowercase letters.

These weak password policies are especially common in self-service portals where users are encouraged to create their own credentials, and they frequently default to easily guessable passwords for convenience.

Susceptibility to Brute-Force Attacks

External systems exposed to the internet are prime targets for brute-force attacks. Attackers use automated tools to try thousands or even millions of username-password combinations until they successfully break into accounts. Without account lockout policies or rate-limiting mechanisms in place, attackers can continue these attempts indefinitely without being detected.

Educational institutions with large user bases (students, faculty, staff) are particularly vulnerable, as the scale of user accounts increases the likelihood that weak or reused passwords exist in the system.

Password Reuse Across Multiple Platforms

Many users reuse passwords across multiple systems, both internal and external. If an attacker gains access to an external system with weak password protection, they can often use the same credentials to attempt access on other systems, such as email, cloud services, or internal networks.

Password reuse makes credential stuffing attacks—where attackers use known username-password pairs from previous breaches—an effective method to compromise accounts on multiple platforms, especially if users have not been forced to adopt unique, strong passwords.

Failure to Implement Account Lockout or Rate Limiting

Without account lockout policies, external systems allow attackers to make repeated login attempts without consequences. In some cases, institutions do not implement rate limiting, allowing brute-force attacks to be executed at high speed. This gives attackers unlimited opportunities to attempt login combinations until they are successful.

During penetration testing, it was found that many external portals allowed unlimited login attempts, increasing the likelihood that brute-force methods would succeed.

Recommendations

To mitigate the risks associated with weak password management on external portals and web applications, institutions should implement the following security measures:

Enforce Strong Password Policies

Implement strong password policies for all external-facing systems. Require a minimum password length (at least 12 characters) and enforce complexity requirements, including the use of uppercase and lowercase letters, numbers, and special characters.

Prevent users from selecting common passwords by implementing a password blacklist that disallows easily guessable passwords (e.g., “password123,” “University2023,” or simple numeric sequences).

Enable Account Lockout and Rate Limiting

Apply account lockout policies that temporarily lock accounts after a set number of failed login attempts (e.g., five attempts). This will help prevent attackers from repeatedly attempting to brute-force their way into accounts.

Implement rate limiting on login pages to slow down the speed of automated brute-force attacks. Rate limiting should introduce delays or CAPTCHAs after several failed attempts to slow down attackers.

Require Multi-Factor Authentication (MFA)

Enforce MFA for all external-facing systems, especially those handling sensitive information such as student data, financial records, or research materials. By requiring a second form of authentication, such as a mobile app or SMS-based code, institutions can significantly reduce the likelihood of account compromise through brute-force attacks.

Ensure that MFA is mandatory for all users, including students, staff, and faculty, to prevent bypassing of this critical security layer.

Monitor and Block Brute-Force Attack Attempts

Use intrusion detection systems (IDS) and web application firewalls (WAFs) to monitor external login attempts and detect suspicious login patterns indicative of brute-force attacks. Set up alerts to notify security teams of unusual login activity, such as multiple failed attempts from the same IP address or repeated login attempts targeting multiple accounts.

Implement geo-blocking or IP blacklisting to prevent login attempts from known malicious regions or IP addresses that are frequently used in brute-force attacks.

Educate Users on Password Hygiene

Conduct regular security awareness training for students, faculty, and staff on the importance of strong password hygiene. Emphasize the risks of using weak or reused passwords and provide guidelines on how to create strong, unique passwords for each system they access.

Encourage the use of password managers, which can help users generate and store complex passwords without the need to remember them manually.

Regularly Audit and Pen-Test External Systems

Perform regular audits of external systems and web applications to ensure password policies are being enforced properly and that there are no gaps in security. Regular penetration testing should be conducted to identify potential weaknesses in external authentication mechanisms, such as the absence of MFA or account lockout policies.

By enforcing strong password policies, implementing MFA, and taking proactive steps to detect and block brute-force attacks, institutions can significantly reduce the risk of account compromise through weak password management on external systems. This will help protect critical resources, including sensitive student and faculty data, from unauthorized access.

Outdated Web Components

Summary

Many schools rely on outdated or unsupported web components, such as old JavaScript libraries and other client-side frameworks, in their external-facing websites and web applications. These components often contain known vulnerabilities that are actively targeted by attackers to compromise both users and the systems they access. Without regular updates and proper patch management, these outdated components leave institutions exposed to a wide range of client-side attacks, including Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and code injection attacks.

Details

Use of Outdated JavaScript Libraries

Many institutions' web applications rely on older versions of JavaScript libraries, such as jQuery, AngularJS, or React, that are no longer maintained or have unpatched security vulnerabilities. Attackers can easily identify and exploit these vulnerabilities using automated tools that scan websites for outdated libraries.

For example, unpatched versions of jQuery have well-documented vulnerabilities that can be exploited to perform Cross-Site Scripting (XSS) attacks. These vulnerabilities allow attackers to inject malicious code into web pages viewed by users, potentially stealing their credentials or installing malware on their devices.

Vulnerabilities in Client-Side Frameworks

Outdated client-side frameworks, such as Bootstrap or Vue.js, also present a major risk when they are not regularly updated. These frameworks are responsible for rendering web pages and handling user interactions, making them an attractive target for attackers.

Attackers can exploit known vulnerabilities in these frameworks to launch attacks that compromise user sessions, manipulate web content, or escalate privileges. Additionally, if security patches are not applied promptly, attackers can use these weaknesses to bypass authentication mechanisms or gain unauthorized access to sensitive data.

Dependency Management Issues

Web applications often include multiple third-party libraries and dependencies that are not actively managed or monitored for updates. These components are commonly bundled together and deployed without adequate security review, increasing the attack surface.

Many institutions fail to properly track which versions of libraries or dependencies are in use, leading to a situation where vulnerable components remain deployed long after patches or updates have been released. This creates a long-term risk, as attackers frequently exploit known vulnerabilities in outdated dependencies.

Increased Exposure to Client-Side Attacks

The presence of outdated web components exposes institutions to client-side attacks such as Cross-Site Scripting (XSS), where attackers inject malicious scripts into web pages. These scripts can steal session cookies, hijack user accounts, or deliver malware to unsuspecting user. Outdated web components also increase the risk of Cross-Site Request Forgery (CSRF), where attackers trick users into unknowingly submitting unauthorized requests on behalf of their active session, potentially compromising their accounts or systems.

Lack of Routine Security Audits for Web Components

Many educational institutions do not conduct regular security audits of their web components or check for outdated libraries. Without proper auditing, it's difficult to identify which components need to be updated or replaced, leaving known vulnerabilities unaddressed.

Web applications are often developed and maintained by different teams, leading to inconsistent patch management and outdated components being left in production environments long after their vulnerabilities are disclosed.

Recommendations

To mitigate the risks posed by outdated web components and client-side vulnerabilities, educational institutions should implement the following measures:

Regularly Update Web Components and Libraries

Ensure that all web components, including JavaScript libraries (e.g., jQuery, React, AngularJS) and client-side frameworks (e.g., Bootstrap, Vue.js), are regularly updated to the latest versions. Updates should include not only feature improvements but also critical security patches that address known vulnerabilities.

Implement a routine patch management process for web components and establish a system for tracking the versions of all third-party libraries used in web applications. This will ensure that outdated libraries are identified and updated promptly.

Conduct Regular Security Audits and Code Reviews

Perform regular security audits and code reviews of web applications to identify and address outdated or vulnerable components. This should include checking for outdated libraries, third-party dependencies, and frameworks that may contain security flaws.

Include security-focused penetration testing in the auditing process to assess the application's resilience against common client-side attacks like XSS and CSRF. This testing will help identify potential weaknesses before attackers can exploit them.

Implement Content Security Policy (CSP)

To mitigate the impact of Cross-Site Scripting (XSS) attacks, implement Content Security Policy (CSP) headers in all web applications. CSP helps prevent the execution of unauthorized scripts by specifying the trusted sources from which the browser can load content.

Enforce strict CSP policies that limit the use of inline scripts and prevent loading of external resources from untrusted domains, thereby reducing the attack surface for client-side vulnerabilities.

Isolate Critical Web Components

For web applications that handle sensitive data or critical services (such as student portals or financial systems), consider isolating critical components in separate containers or environments. This reduces the risk of outdated components compromising the entire system and limits the potential damage if an attack is successful.

Ensure that these isolated components are subject to stricter security controls, including regular patching, stricter authentication measures, and enhanced monitoring for suspicious activity.

Monitor and Block Exploit Attempts

Use Web Application Firewalls (WAFs) to monitor and block attempts to exploit known vulnerabilities in outdated web components. A WAF can detect and block malicious requests, such as those targeting XSS or CSRF vulnerabilities, even if the underlying web application contains flaws.

Set up real-time monitoring and alerting for unusual traffic patterns or exploit attempts targeting outdated components. This will allow security teams to respond quickly to potential breaches or attacks in progress.

By regularly updating web components, implementing security-focused monitoring tools, and conducting routine audits, institutions can significantly reduce the risk of client-side attacks exploiting outdated libraries. These measures will help protect both users and systems from being compromised through vulnerabilities in external-facing applications.

Directory Indexing Enabled

Summary

A number of schools suffer from improper server configurations, such as directory indexing being enabled on their web servers. This misconfiguration allows attackers to easily browse and access file directories that are meant to be hidden from public view. When directory indexing is enabled, it can expose sensitive information or files that provide attackers with valuable insights into an institution's internal structure, web application components, and security posture. This can lead to information disclosure, which attackers can leverage for further exploitation or reconnaissance.

Details

Exposure of Sensitive Information

Directory indexing occurs when a web server is configured to list the contents of a directory if no default file (like index.html) is present. When enabled, users and attackers alike can access a list of files and directories on the server, including sensitive information like configuration files, logs, backup files, or even files containing credentials.

During penetration testing, many institutions were found to have publicly accessible directories that exposed configuration files (config.php, .env), old backups, or temporary files (backup.sql, test.zip) that could be used to extract sensitive data like database credentials or API keys.

Reconnaissance and System Mapping

Attackers can use directory indexing to perform reconnaissance, gaining insight into the structure of an institution's web applications and file storage systems. By browsing through available directories, attackers can identify software versions, installed plugins, and third-party components used by the institution, which they can then research for known vulnerabilities.

This exposure can also reveal internal naming conventions and development practices, offering attackers clues about where important files may be located, or how to craft more targeted attacks.

Exploitation of Misplaced or Unsecured Files

Institutions often inadvertently leave behind files that were intended for internal use only. These files could include development notes, debugging logs, or obsolete but sensitive files that are no longer in use but still accessible. Attackers can access these files to gather more intelligence or directly exploit the information they contain.

In some cases, attackers find unsecured scripts or executables that can be manipulated to gain unauthorized access to internal systems. For example, an improperly configured admin script left on the server may allow attackers to bypass authentication mechanisms or gain elevated privileges.

Potential for Information Disclosure

Directory indexing can inadvertently disclose the existence of files that would otherwise remain hidden. For example, seeing files like admin_backup.tar.gz or user_data.sql in an indexed directory can reveal the presence of sensitive data and provide a direct target for attackers.

Even seemingly innocuous files can give away crucial security details, such as version information for CMS platforms or security libraries, which attackers can use to tailor their attacks or find unpatched vulnerabilities.

Recommendations

To mitigate the risks associated with directory indexing, schools should take the following measures:

Disable Directory Indexing by Default

Ensure that directory indexing is disabled on all web servers by default. This can be done by modifying the server configuration file (such as .htaccess for Apache or nginx.conf for NGINX) to disallow directory listings. For example:

Conduct regular reviews of web server configurations to ensure directory indexing remains disabled.

Audit Public-Facing Directories

Conduct a thorough audit of all public-facing directories to ensure no sensitive files or unnecessary files are exposed to users. Remove or relocate any files that should not be accessible from the web, such as:

- Configuration files (e.g., config.php, .env)
- Backup files (e.g., backup.sql, db_backup.zip)]
- Temporary or debugging files (e.g., test.php, debug.log)

Ensure that critical files are located in non-public directories and are protected by proper access control mechanisms.

Use Strict Access Controls

Implement role-based access control (RBAC) to ensure that only authorized personnel have access to sensitive files and directories. Use directory permissions to restrict access to critical folders and files, ensuring that even if directory indexing is mistakenly enabled, unauthorized users cannot access protected resources.

For sensitive admin directories, consider restricting access by IP address or using Multi-Factor Authentication (MFA) for additional security.

Implement Security Headers and Response Codes

Use security headers to minimize the exposure of sensitive resources. For instance, the X-Content-Type-Options header can prevent certain types of content from being rendered inappropriately, while the X-Frame-Options header can mitigate clickjacking attacks.

Ensure that proper HTTP response codes are returned when users attempt to access restricted directories. For example, directories that should not be browsed should return a 403 Forbidden error instead of listing the contents.

Regularly Monitor for Directory Indexing

Use automated scanning tools to monitor for instances of directory indexing across web servers. Tools like OWASP ZAP, Nikto, or Burp Suite can help detect when directory indexing is enabled and identify which directories are exposed.

Regularly run scans to ensure no new instances of directory indexing are accidentally introduced during system updates or configuration changes.

Implement a Web Application Firewall (WAF)

Deploy a Web Application Firewall (WAF) to filter out malicious requests and prevent attackers from exploiting directory indexing. A WAF can detect and block automated tools that scan for exposed directories and files, reducing the risk of exploitation.

Ensure the WAF is properly configured to inspect web traffic and alert administrators of any unusual activity, such as repeated attempts to access directory listings.

Weak SSL/TLS Protocols

Summary

Several educational institutions continue to use outdated or weak SSL/TLS encryption protocols to secure communications between users and servers. These outdated protocols, such as SSLv2, SSLv3, or weak versions of TLS (e.g., TLS 1.0, TLS 1.1), leave connections vulnerable to man-in-the-middle (MitM) attacks, downgrade attacks, and data interception. Without the proper enforcement of strong encryption standards, attackers can exploit these weaknesses to decrypt sensitive data in transit, manipulate the integrity of communications, or impersonate legitimate services.

Details

Use of Outdated SSL/TLS Versions

Many institutions were found to be using deprecated SSL/TLS protocols, such as SSLv2 and SSLv3, or older versions of TLS like TLS 1.0 and TLS 1.1. These protocols are vulnerable to known exploits, such as the POODLE attack (Padding Oracle On Downgraded Legacy Encryption) and the BEAST attack (Browser Exploit Against SSL/TLS).

These protocols are considered insecure due to their weak encryption algorithms and vulnerabilities to cipher block chaining (CBC) and downgrade attacks. Attackers can exploit these weaknesses to decrypt communications and intercept sensitive data, such as login credentials, session tokens, or personal information transmitted between users and the institution's servers.

Weak Cipher Suites and Poor Encryption Settings

Even when newer versions of TLS (e.g., TLS 1.2, TLS 1.3) are in use, institutions often allow the use of weak cipher suites, such as RC4 or 3DES, which are no longer considered secure. These weak ciphers can be cracked by attackers using modern computational techniques, enabling them to decrypt data in real-time or conduct session hijacking.

Poor configurations, such as the acceptance of weak key lengths or improper certificate management, further degrade the security of SSL/TLS implementations. This can result in incomplete encryption, leaving parts of the communication unprotected and vulnerable to attack.

Vulnerability to Man-in-the-Middle (MitM) Attacks

Outdated or weak SSL/TLS configurations make institutions susceptible to man-in-the-middle (MitM) attacks, where an attacker intercepts and relays communications between a user and the server. If weak SSL/TLS protocols are used, the attacker can decrypt the intercepted traffic and gain access to sensitive data or modify the data in transit.

In some cases, attackers may perform downgrade attacks, forcing the server to use a weaker, vulnerable SSL/TLS protocol version or cipher, allowing them to decrypt or tamper with the communication. This is especially dangerous when sensitive transactions, such as login attempts or financial information exchanges, are involved.

Non-Compliance with Modern Security Standards

The continued use of weak SSL/TLS protocols violates modern security standards, such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and other regulations that require the use of strong encryption for sensitive data transmission.

Institutions that fail to update their SSL/TLS configurations may face compliance issues, which could result in regulatory fines, loss of accreditation, or reputational damage in the event of a data breach.

Lack of Certificate and Key Management Best Practices

Improper management of SSL certificates, such as the use of self-signed certificates, expired certificates, or certificates with weak cryptographic algorithms, further weakens the security of SSL/TLS implementations. Attackers can exploit these weaknesses to impersonate legitimate servers or intercept encrypted communications.

Failing to follow proper certificate pinning practices increases the risk of MitM attacks, as attackers can trick users into trusting malicious or forged certificates.

Recommendations

To mitigate the risks posed by weak SSL/TLS protocols, educational institutions should take the following steps:

Disable Deprecated SSL/TLS Versions

Disable outdated and insecure SSL/TLS versions, such as SSLv2, SSLv3, TLS 1.0, and TLS 1.1, across all servers and applications. Only allow TLS 1.2 and TLS 1.3, which provide strong encryption and are resistant to known vulnerabilities.

Modify server configuration files (such as nginx.conf for NGINX or httpd.conf for Apache) to restrict the allowed SSL/TLS versions.

Conduct regular reviews of SSL/TLS settings to ensure they are in line with current security standards.

Enforce Strong Cipher Suites

Only allow the use of strong cipher suites, such as AES-GCM and ChaCha20, and disallow weak ciphers like RC4 or 3DES. Configure web servers to prioritize modern encryption algorithms that provide both confidentiality and integrity.

Regularly audit cipher suites to ensure they meet modern security requirements, and adjust configurations as new vulnerabilities are discovered.

Implement Strict Certificate and Key Management

Use trusted certificate authorities (CAs) to issue SSL/TLS certificates, and avoid the use of self-signed certificates on public-facing systems. Ensure that all certificates are valid, not expired, and use strong encryption algorithms, such as SHA-256 or higher.

Implement certificate pinning to ensure that clients only accept trusted certificates from known sources, reducing the risk of MitM attacks using forged certificates.

Regularly rotate SSL/TLS certificates and private keys to reduce the risk of long-term exposure and compromise.

Enable HTTP Strict Transport Security (HSTS)

Implement HTTP Strict Transport Security (HSTS) headers to enforce secure HTTPS connections between users and servers. This prevents browsers from connecting to a server over an insecure HTTP connection, mitigating the risk of MitM attacks. This ensures that all communications between users and the institution's servers are encrypted and prevents downgrades to insecure protocols.

Conduct Regular Security Audits

Perform regular security audits of SSL/TLS configurations across all servers and web applications. Use tools like Qualys SSL Labs, OpenSSL, or testssl.sh to identify weak protocols, outdated cipher suites, and other misconfigurations that may expose the system to attack.

Monitor for SSL/TLS Attacks

Implement Intrusion Detection Systems (IDS) and Web Application Firewalls (WAFs) to monitor for SSL/TLS attacks, such as downgrade attempts or MitM attacks. Set up alerts for any suspicious activity involving SSL/TLS handshakes or unauthorized certificate usage.

Missing Security Headers

Summary

Missing essential security headers was a problem across the board, leaving schools vulnerable to common web-based attacks such as Cross-Site Scripting (XSS), Clickjacking, and Content Injection. These headers are a simple yet effective way to improve the security of web applications by controlling how browsers handle and interpret web content. The absence of key headers increases the risk of user data exposure and exploitation through various client-side attacks, which could compromise both users and the institution's systems.

Details

Lack of Content Security Policy (CSP)

One of the most critical missing security headers is the Content Security Policy (CSP). CSP helps mitigate Cross-Site Scripting (XSS) and other code injection attacks by restricting which sources are allowed to load resources such as scripts, styles, and media on a web page.

Without CSP, attackers can inject malicious scripts into the website, potentially stealing session cookies, hijacking user accounts, or executing malicious code within users' browsers. During penetration testing, it was found that many institutional websites did not implement any form of CSP, leaving them exposed to XSS attacks.

Absence of HTTP Strict Transport Security (HSTS)

The lack of HTTP Strict Transport Security (HSTS) headers makes websites vulnerable to man-in-the-middle (MitM) attacks. HSTS forces browsers to always use HTTPS connections, ensuring that communications between the server and the user are encrypted and preventing attackers from downgrading connections to insecure HTTP.

Without HSTS, attackers can intercept unencrypted traffic and potentially steal sensitive information, such as login credentials, or inject malicious content into the web page. Many institutional websites were found to lack HSTS headers, making it possible for attackers to exploit insecure connections.

Missing X-Content-Type-Options Header

The X-Content-Type-Options header is used to prevent browsers from interpreting files as a different type than what is specified by the server, a technique often exploited in content-type sniffing attacks. For example, attackers may attempt to upload a file that appears benign (like a text file) but is interpreted as executable code by the browser.

Without this header, attackers can exploit the browser's ability to guess the content type and execute malicious scripts or files. Several educational institutions were found to be missing this header, leaving them exposed to potential code execution vulnerabilities.

Absence of X-Frame-Options Header

The X-Frame-Options header prevents Clickjacking attacks by disallowing the website from being embedded in an iframe on another site. Clickjacking tricks users into clicking on something different than what they perceive, such as invisible buttons or links, which can lead to unintended actions, including sharing sensitive data.

Without this header, attackers can embed an institution's website in an iframe and trick users into performing unintended actions. During security reviews, many websites did not have the X-Frame-Options header set, making them vulnerable to clickjacking attacks.

Missing Referrer-Policy Header

The Referrer-Policy header controls how much referrer information is shared when users navigate between websites. Without this header, sensitive information such as full URLs containing personal data or session identifiers may be exposed to third-party websites, creating privacy and security risks.

Many institutions were found to be missing this header, which could lead to inadvertent information disclosure to untrusted or external sites.

Lack of Cross-Origin Resource Sharing (CORS) Policy

The absence of proper CORS policies can allow malicious websites to make unauthorized requests to an institution's web applications. Cross-Origin Resource Sharing (CORS) defines which domains are allowed to interact with resources from a different domain, ensuring that external sites cannot access restricted content.

Without CORS restrictions, attackers can exploit vulnerabilities to steal sensitive data or perform unauthorized actions across different domains. Many educational websites lacked appropriate CORS policies, leading to potential exposure to Cross-Site Request Forgery (CSRF) attacks and data leakage.

Recommendations

To reduce the risks posed by missing security headers, educational institutions should implement the following security measures:

Implement a Content Security Policy (CSP)

Deploy a Content Security Policy (CSP) header to mitigate XSS and other client-side attacks. The CSP should specify trusted sources for scripts, styles, images, and other resources, limiting the risk of malicious code being injected into web pages.

Regularly review and update the CSP to reflect changes in the website's structure and requirements, ensuring that only trusted resources are allowed to load.

Enable HTTP Strict Transport Security (HSTS)

Enforce secure HTTPS connections by implementing the HSTS header. This ensures that all future requests to the institution's website are made over encrypted HTTPS connections, preventing MitM attacks.

Apply HSTS to all subdomains to protect the entire web infrastructure from insecure HTTP traffic.

Set the X-Content-Type-Options Header

Add the X-Content-Type-Options header with the value nosniff to prevent browsers from guessing the MIME type of a file. This reduces the risk of attackers exploiting content-type sniffing vulnerabilities.

Use the X-Frame-Options Header to Prevent Clickjacking

Protect against Clickjacking by adding the X-Frame-Options header, which prevents your website from being embedded in an iframe on another domain. The recommended setting is:

Implement the Referrer-Policy Header

Add the Referrer-Policy header to control how much referrer information is shared when users navigate away from your site. A strict policy helps protect user privacy and prevent unintentional exposure of sensitive information:

Configure Cross-Origin Resource Sharing (CORS)

Set a CORS policy to define which domains are permitted to make cross-origin requests to your web applications. This helps prevent unauthorized external sites from accessing your resources:

By implementing these security headers and regularly auditing their presence and configuration, institutions can greatly improve the security of their web applications. These simple yet powerful measures protect users from common attacks, ensure secure communication, and minimize the risk of data breaches or compromises.

Cloud Vulnerabilities

As more schools migrate to cloud-based systems, security gaps in cloud configurations become a significant concern. The following vulnerabilities were common across most schools:

Cloud Methodology

Cloud testing begins with reconnaissance and asset discovery. This phase involves identifying all public-facing assets associated with the cloud environment, such as storage buckets, virtual machines, or containers. DNS enumeration and port scanning are employed to map out cloud services and APIs, looking for exposed endpoints. Additionally, testers review metadata endpoints, which are often accessible in cloud environments, to gather information about the instance and connected services.

In the exploitation phase, testers focus on misconfigurations and vulnerabilities in cloud-specific services. Common issues include improperly configured storage buckets, overly permissive IAM (Identity and Access Management) roles, or vulnerable APIs.

We leverage these weaknesses to gain unauthorized access to sensitive data or escalate privileges within the cloud environment. This phase also includes testing for privilege escalation, lateral movement between cloud services, and examining external APIs for weak authentication.

The post-exploitation and reporting phase involves evaluating the impact of a successful compromise, such as data extraction, network persistence, and the potential for further attacks. We document the attack path, from asset discovery to exploitation, along with any sensitive data accessed.

Weak Password Management in Cloud Systems

Summary

Many of the cloud environments we tested suffered from weak password management, where inadequate password policies and the lack of account lockout mechanisms leave cloud accounts vulnerable to brute-force or password-spraying attacks. Attackers can exploit these weaknesses to repeatedly attempt login combinations, leading to unauthorized access to sensitive resources hosted in the cloud. Without stringent password policies and protections, cloud systems become easy targets for credential-based attacks, which can compromise critical data, infrastructure, and services.

Details

Inadequate Password Policies

Many cloud platforms and applications fail to enforce strong password policies, allowing users to set weak or easily guessable passwords, such as “Password123” or “Welcome2024.” These weak passwords increase the risk of unauthorized access.

Some environments lack mandatory password complexity requirements (e.g., requiring uppercase, lowercase, numbers, and special characters) or minimum length enforcement, leaving accounts susceptible to simple brute-force attacks.

No Account Lockout or Rate Limiting

A common issue in cloud environments is the absence of account lockout thresholds. Without account lockouts, attackers can attempt to log in using various password combinations without restriction.

Password spraying is particularly effective in environments lacking account lockout policies, as attackers can try common passwords across many accounts, bypassing detection.

Credential Reuse Across Cloud and On-Prem Systems

Users often reuse passwords across multiple platforms, including cloud systems and on-premises applications. If a password is compromised in one system, attackers can use it to access other accounts, particularly in hybrid environments.

Inconsistent Password Policy Enforcement Across Cloud Platforms

In multi-cloud environments, password policies are often inconsistent across platforms, leading to a fragmented security posture that attackers can exploit by focusing on weaker systems.

Recommendations

Enforce Strong Password Policies

Enforce strong password policies, including minimum password lengths and complexity requirements, across all cloud accounts.

Periodically review and update password policies to reflect evolving security standards and industry best practices.

Implement Account Lockout and Rate Limiting

Configure account lockout mechanisms to limit failed login attempts, and implement rate limiting to slow down brute-force attacks.

Enable Monitoring for Password-Based Attacks

Implement cloud-native monitoring tools to detect and respond to brute-force and password-spraying attacks, and set up alerts for repeated failed login attempts.

Educate Users on Strong Password Hygiene

Provide ongoing security awareness training on password best practices, and encourage the use of password managers to avoid reuse.

By enforcing strong password policies and applying account lockout mechanisms, institutions can significantly reduce the risk of cloud account compromises due to password-based attacks. Proper password management is essential to securing cloud environments and protecting sensitive resources from unauthorized access.

Multi-Factor Authentication (MFA) Not Configured

Summary

In many cloud environments, Multi-Factor Authentication (MFA) is not configured for privileged accounts and regular user accounts. This omission leaves accounts vulnerable to phishing, credential-stuffing, and other password-based attacks. Without MFA, attackers who successfully compromise a password can gain full access to critical cloud resources, bypassing a vital security layer.

Details

MFA Not Configured for Privileged Accounts

Privileged accounts, such as those held by administrators, are often not protected by MFA. This creates a significant security gap, as these accounts typically have broad access to cloud infrastructure and sensitive data.

MFA Not Configured for User Accounts

In addition to privileged accounts, many standard user accounts lack MFA protection, increasing the risk of unauthorized access, particularly in the case of credential-stuffing or phishing attacks.

Vulnerability to Phishing and Credential-Stuffing Attacks

Without MFA, attackers can easily compromise accounts through phishing or credential-stuffing, gaining full access without needing a second factor for authentication.

Recommendations

Enforce MFA Across All Accounts

Require MFA for all cloud accounts, particularly for administrative and privileged accounts, to prevent unauthorized access through compromised credentials.

Support Multiple MFA Methods

Offer a range of MFA options (e.g., TOTP, hardware tokens) to ensure broad adoption and user convenience.

Monitor MFA Compliance

Regularly audit MFA enrolment and enforce compliance through automated policies where possible.

By enabling MFA for all users, particularly privileged accounts, cloud environments can drastically reduce the risk of compromise from password-based attacks. MFA provides an essential security layer that is critical for protecting sensitive accounts.

Missing Conditional Access Policies

Summary

Conditional Access Policies, which enforce additional security controls based on the context of login attempts, such as location, device, or risk level were insufficient or completely missing. Without these policies, cloud environments are more susceptible to unauthorized access, especially from high-risk logins originating from outside trusted locations, such as outside Australia.

Details

No Conditional Access for High-Risk Logins

Cloud environments often lack the enforcement of MFA or additional verification for high-risk logins, such as those from unfamiliar locations or devices.

No Location-Based Restrictions

Without geographic access controls, logins from risky locations (e.g., outside trusted countries like Australia) are not blocked or challenged, leaving the cloud environment vulnerable to unauthorized access.

Lack of Application-Specific Controls

Conditional Access Policies that enforce additional verification based on application sensitivity are often missing, leading to inadequate protection for sensitive resources.

Recommendations

Implement Conditional Access Policies

Enforce policies that require MFA for high-risk logins and set location-based restrictions for sensitive access.

Apply Application-Specific Policies

Define policies based on the sensitivity of applications, requiring additional security measures for critical systems.

Regularly Review Access Policies

Continuously update policies to reflect changing threats and access patterns.

Conditional Access Policies are crucial for enforcing risk-based security controls, helping to secure cloud environments from unauthorized access based on the context of login attempts.

Unmanaged Accounts and Devices

Summary

The presence of inactive user accounts, unmanaged guest access, and untracked devices increases the attack surface in cloud environments. Dormant accounts and unmanaged devices are prime targets for attackers, allowing them to infiltrate cloud environments and move laterally to escalate privileges or exfiltrate data.

Details

Inactive Accounts

Many cloud environments contain inactive accounts that have not been used for extended periods. Attackers can exploit these dormant accounts to gain unauthorized access, especially if they are not protected by MFA.

Unmanaged Guest Accounts

Guest accounts are often left active long after they are no longer needed, providing attackers with entry points into the cloud environment.

Untracked Devices

The lack of device management allows compromised or unverified devices to access cloud resources without oversight.

Recommendations

Audit and Remove Inactive Accounts

Regularly audit and remove inactive accounts to minimize attack vectors.

Manage Guest Access

Implement policies that automatically expire guest accounts after a set period.

Enforce Device Management

Require all devices connecting to the cloud to be registered and verified.

By regularly auditing accounts and devices, institutions can reduce the risk of unauthorized access through dormant accounts or unmanaged assets, ensuring better protection for cloud environments.

Excessive User Permissions

Summary

In many of the cloud environments we tested, non-administrative users are granted excessive permissions, such as the ability to create custom applications or register tenants. This over-permissioning increases the risk of privilege escalation or the introduction of malicious software, as attackers who gain access to these accounts can abuse the elevated permissions to compromise the cloud environment.

Details

Non-Admin Users Can Register Applications

Some environments allow non-admin users to register custom applications, which attackers can exploit to deploy malicious applications.

Non-Admin Users Can Create Tenants

In certain cloud platforms, non-admins are able to create new tenants, which attackers can use to bypass existing security controls.

Recommendations

Restrict Permissions for Non-Admin Users

Limit application registration and tenant creation to admin users only.

Audit Permissions Regularly

Continuously review user permissions and adjust to prevent over-permissioning.

By restricting excessive permissions and regularly auditing user roles, cloud environments can prevent privilege escalation and the unauthorized deployment of applications.

These vulnerabilities, if left unresolved, expose institutions to a range of threats, including brute-force attacks, credential-stuffing, unauthorized access, and privilege escalation. Enforcing strong password policies, applying MFA across all accounts, managing inactive and guest accounts, and restricting excessive user permissions are critical steps in mitigating these risks.

In addition, implementing Conditional Access Policies to enforce location-based restrictions and high-risk login controls, along with device management, will significantly reduce the attack surface. Institutions that proactively address these issues will be better equipped to defend against cyberattacks, protecting their sensitive data and cloud infrastructure. Failure to address these gaps not only increases the likelihood of successful attacks but also drives up the costs of breaches, a burden that continues to grow year after year.

Impact of findings:

Data Breaches

The vulnerabilities identified in the penetration tests, particularly weak password management, outdated systems, and cloud misconfigurations, greatly increase the likelihood of unauthorized access to sensitive data. Educational institutions store vast amounts of Personally Identifiable Information (PII), including student records, staff credentials, and financial data. In addition, intellectual property (IP) such as research outputs are valuable targets for cybercriminals. Data breaches in this sector have the potential to:

- Expose PII, leading to identity theft and personal risks for students, faculty, and staff.
- Compromise intellectual property, potentially harming research partnerships and innovation efforts.
- Increase the likelihood of secondary attacks, where compromised data is used for future breaches or sold on the black market.

Operational Disruptions

Schools depend heavily on digital platforms for both academic and administrative operations. Vulnerabilities in SMB protocols, outdated servers, and misconfigured cloud environments create the risk of severe operational disruptions. Breaches exploiting these weaknesses can result in:

- System outages that prevent access to learning management systems (LMS), enrolment platforms, and research databases, halting daily operations.
- Interruption of learning activities, causing classes to be cancelled or delayed and limiting students' access to essential resources for assignments and exams.
- Loss of critical research data, particularly for universities with ongoing research projects, potentially resulting in loss of years of work or disruption of funded research programs.

Financial Losses

Data breaches can result in hefty costs, including incident response, system restoration, and legal fees. For example, the ransomware attack on the University of Newcastle led to an estimated $3.2 million in losses due to system downtime, recovery efforts, and reputational damage. The 2024 Cost of a Data Breach Report places the average cost of a breach in the Australian education sector at AUD 4.14 million, with some breaches costing upwards of AUD 7.46 million when significant operational disruptions occur.

Costs of Non-Compliance: Institutions that fail to comply with data privacy laws such as Australia's Privacy Act 1988 may face regulatory fines, lawsuits, and damage to their reputations. In 2023, an Australian university faced significant penalties for failing to report a data breach that exposed the personal information of over 5,000 students.

These costs are influenced by several factors:

- Incident Response and System Restoration: Recovering from a breach can take months, requiring a significant investment in incident response, including forensic analysis, system repairs, and restoring access to services.
- Legal Liabilities: In the event of a data breach involving PII, educational institutions may face legal consequences under regulations such as the Privacy Act 1988. This can include fines, lawsuits, and regulatory penalties.
- Ransom Payments: In the case of ransomware attacks, institutions may face ransom demands to regain access to encrypted files. Even when law enforcement is involved, there may still be a financial cost related to system recovery.

Reputational Damage

A publicized breach can erode trust in an institution's ability to protect sensitive information. For example, following a data breach, enrolment rates at a Melbourne-based university dropped by 8%, with prospective students citing concerns about data security. Similarly, partnerships with research institutions may be jeopardized if the institution is perceived as having inadequate cybersecurity measures.

The effects of reputational damage can have long-term consequences, including:

- Erosion of Trust: Students, parents, faculty, and alumni may lose trust in the institution's ability to protect sensitive information, leading to reputational harm that could take years to recover from.
- Declining Enrolment: Potential students may be deterred from applying to institutions that have suffered a data breach, especially if they fear for the security of their personal data. This could lead to reduced enrolment rates, affecting both tuition revenue and institutional growth.
- Loss of Funding Opportunities: Research institutions rely on grants and partnerships, which could be jeopardized if the organization is seen as a security risk. Funding bodies may be less willing to allocate resources to institutions with a poor cybersecurity track record.
- Impact on Partnerships: Educational institutions often collaborate with industry partners, research organizations, and other universities. A major breach could lead to partnerships being reevaluated or terminated due to concerns over data security.

Prolonged Breach Lifecycles and Recovery

As observed in the 2024 Cost of a Data Breach Report, shadow data and decentralized data systems significantly extend the breach lifecycle, making recovery more complex. This poses a unique challenge for educational institutions where multiple systems—on-premise, cloud-based, and third-party services—are often poorly integrated. Extended recovery times increase financial costs and prolong operational downtime, further exacerbating the effects of a breach.

Spartans Security's Recommendations

Strengthen Password Management and Enforce MFA

Weak password management was one of the most prevalent issues found during penetration tests, both internally (with shared, weak passwords such as test123:test123) and externally (with weak password policies for public-facing services). Implementing robust password management policies, along with Multi-Factor Authentication (MFA), is crucial to reducing the risk of credential theft and brute force attacks.

Educational institutions should:

- Enforce strong password policies that require complex passwords for all accounts, particularly privileged ones. This will help prevent Password Spraying and Credential Dumping attacks.
- Implement MFA for all users, including students, staff, and administrative personnel, especially for privileged accounts. MFA will protect against account takeovers and reduce the effectiveness of phishing and credential-stuffing attacks.
- Apply account lockout policies to prevent brute force attempts, a vulnerability highlighted in the pentests.

Patch Legacy Systems and Update Software Regularly

Findings from the pentests highlighted that several systems are running End-of-Life software (e.g., Windows Server 2012) and using old, vulnerable JavaScript libraries on public-facing web applications. These outdated systems are particularly susceptible to exploitation for privilege escalation and remote code execution.

Educational institutions should:

- Regularly patch and update both operating systems and web applications to reduce the risk of Exploitation for Client Execution (T1203).
- Migrate from End-of-Life systems like Windows Server 2012 to newer, supported platforms to close vulnerabilities exploited by attackers.
- Update JavaScript libraries and other third-party software to avoid vulnerabilities that lead to Drive-by Compromise (T1189) and client-side attacks.
- By ensuring that systems are up-to-date, institutions can reduce exposure to known vulnerabilities and mitigate risks related to outdated infrastructure.

Adopt Zero Trust Security Models

The education sector's reliance on cloud platforms, as seen in the pentest findings (e.g., weak password policies and insufficient MFA for privileged accounts), necessitates the adoption of a Zero Trust security model. This approach can:

- Enforce strict authentication and verification processes for every device and user, minimizing risks associated with unmanaged guest accounts and inactive users.
- Implement continuous monitoring of internal network activities, preventing lateral movement across systems when compromised credentials are used.
- Protect against misconfigured Active Directory Certificate Services (ADCS) and outdated systems, both of which were found to be easy entry points for attackers.
- Zero Trust will help secure critical assets, especially in environments where conditional access policies are not enforced, as noted in the cloud findings from the pentests.

Implement Cybersecurity Awareness Training

Based on pentest findings, a large number of the vulnerabilities in the education sector stem from weak password management and improper user practices. Regular cybersecurity training can help reduce risks related to phishing, credential theft, and the improper use of third-party applications.

Training programs should focus on:

- Educating students, faculty, and staff on safe password practices, such as avoiding weak passwords like loreto@123 and test123:test123, and the importance of enabling MFA.
- Identifying phishing attempts and social engineering tactics to prevent credential compromise.
- The proper use of cloud services, with a focus on recognizing the dangers of unmanaged guest accounts and the impact of Shadow IT (such as unsanctioned third-party apps).
- Training should be mandatory and reinforced with regular updates, ensuring staff and students are aware of evolving threats.

Invest in AI and Automation

Findings from the pentests reveal numerous vulnerabilities across internal, external, and cloud environments, especially in weak password management, outdated systems, and misconfigurations in SMB protocols. By deploying AI-driven cybersecurity tools and automating security monitoring, educational institutions can:

- Detect and respond to credential-based attacks (such as Password Spraying and Valid Accounts) in real-time.
- Identify patterns in cloud misconfigurations, particularly those involving MFA and password policies, and automate immediate corrective actions.
- Proactively monitor and flag potential threats, such as exploitation of SMB protocols and End-of-Life operating systems, before they escalate into full-blown breaches.
- The 2024 Cost of a Data Breach Report showed that institutions leveraging AI and automation saved an average of 2.8 million per breach. This emphasizes the importance of using automated solutions to manage cloud and on-premise security environments while reducing human error.

Conclusion

Our penetration tests between 2022 and 2024 uncovered significant common vulnerabilities in the schools we tested, including weak password management, lack of Multi-Factor Authentication (MFA), excessive user permissions, and unmanaged accounts. These issues, combined with reliance on legacy systems and inconsistent security across cloud infrastructures, leave institutions highly vulnerable to data breaches, ransomware, and operational disruptions.

To combat these risks, educational institutions must prioritize enforcing MFA, tightening access controls, and regularly auditing user permissions. Addressing these critical gaps will not only protect sensitive data and cloud resources but also safeguard the operational integrity of these institutions. By taking immediate action, institutions can strengthen their defenses against increasingly sophisticated cyber threats and ensure long-term resilience in the face of a rapidly evolving digital landscape.

SPARTANS SECURITY
YOUR CYBERSECURITY PARTNER