Common Cyber Security Vulnerabilities and Attacks with their Preventive ISM Controls

Based on June 2024 ISM

Last updated: 26 August 2024

Table of Contents

Background

The Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) is a comprehensive set of guidelines and best practices designed to assist Australian government agencies and organisations in managing and protecting their information systems from threats. The ISM provides a framework for establishing and maintaining a strong security posture, addressing a wide range of security controls, from access management to incident response. By following the ISM, organisations can ensure that they are implementing the necessary measures to protect sensitive data and critical infrastructure, in line with national security standards. The ISM is updated quarterly to reflect the evolving threat landscape, making it an essential tool for any organisation committed to maintaining high standards of cyber security.

Purpose

The purpose of this document is to serve as a practical resource for organisations seeking to understand and mitigate common cyber security vulnerabilities through the implementation of relevant controls outlined in the Information Security Manual (ISM). Whether an organisation has already suffered a specific cyber attack and needs to implement corrective measures, or it recognises an increased susceptibility to certain types of threats, this guide provides targeted advice on applying the appropriate ISM controls.

By mapping various cyber attacks to their corresponding preventive ISM controls, this document helps organisations identify gaps in their current security posture and take actionable steps to enhance their cyber environment. It is particularly valuable for organisations looking to respond to incidents, as well as those proactively seeking to secure their systems against potential vulnerabilities. In doing so, it empowers organisations to not only recover from past incidents but also to build resilience against prevalent threats.

Brute Force Attacks

A brute force attack is a method used by attackers to gain unauthorised access to a system by systematically attempting every possible combination of characters until the correct password is found. This type of attack does not rely on any specific knowledge about the password, making it a time-consuming but potentially effective method, especially against weak or short passwords.

Brute force attacks can be automated, with tools that rapidly test numerous combinations, increasing the likelihood of success if passwords are simple or commonly used. To defend against brute force attacks, organisations should enforce strong password policies that require complex, long passwords, implement account lockout policies after a set number of failed login attempts, and use multi-factor authentication (MFA) to add an additional layer of security. These measures make it significantly harder for brute force attacks to succeed.

Control: ISM-1403; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.

Control: ISM-1685; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3

Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.

Control: ISM-1173; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Multi-factor authentication is used to authenticate privileged users of systems.

Control: ISM-0974; Revision: 6; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Multi-factor authentication is used to authenticate unprivileged users of systems.

Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML1, ML2, ML3

Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Dictionary Attacks

A dictionary attack is a method used by attackers to gain unauthorised access to a system by systematically trying every word in a predefined list, known as a dictionary, to guess passwords or passphrases. This type of attack takes advantage of the tendency of some users to choose common or simple passwords that can be found in such dictionaries. Unlike brute force attacks, which attempt every possible combination of characters, dictionary attacks are more targeted and efficient because they rely on likely password choices.

To defend against dictionary attacks, it's important to use complex, unpredictable passwords or passphrases that are long and include a mix of characters. Implementing account lockout policies after a certain number of failed login attempts and encouraging the use of multi-factor authentication (MFA), can significantly reduce the likelihood of a successful attack.

Control: ISM-0421; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.

Control: ISM-1557; Revision: 2; Updated: Dec-21; Applicability: S; Essential Eight: N/A

Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.

Control: ISM-0422; Revision: 8; Updated: Dec-21; Applicability: TS; Essential Eight: N/A

Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.

Control: ISM-1558; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature or any other publicly available material.

Control: ISM-1403; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.

Control: ISM-1590; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Credentials are changed if:

- they are compromised
- they are suspected of being compromised
- they are discovered stored on networks in the clear
- they are discovered being transferred across networks in the clear
- membership of a shared account changes
- they have not been changed in the past 12 months.

Phishing Attacks

Phishing attacks are a common form of cyber-attack where threat actors attempt to trick individuals into revealing sensitive information, such as passwords or financial details, by masquerading as a trustworthy entity. These attacks often involve fraudulent emails, text messages, or websites that appear legitimate but are designed to deceive the victim. The messages typically create a sense of urgency, such as claiming that an account has been compromised, prompting the recipient to act quickly without verifying the authenticity of the communication.

The consequences of falling for a phishing attack can be severe, including identity theft, financial loss, and unauthorised access to personal or corporate accounts. To defend against phishing, it is crucial to educate users about recognising suspicious communications, implement email filtering, and use multi-factor authentication to add an extra layer of security.

Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Cyber security awareness training is undertaken annually by all personnel and covers:

- the purpose of the cyber security awareness training
- security appointments and contacts
- authorised use of systems and their resources

- protection of systems and their resources
- reporting of cyber security incidents and suspected compromises of systems and their resources.

Control: ISM-1502; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Emails arriving via an external connection where the email source address uses an internal domain, or internal subdomain, are blocked at the email gateway.

Control: ISM-1540; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

DMARC records are configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.

Control: ISM-1234; Revision: 5; Updated: Dec-22; Applicability: All; Essential Eight: N/A

Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.

Control: ISM-0569; Revision: 5; Updated: Jun-22; Applicability: All; Essential Eight: N/A

Emails are routed via centralised email gateways.

Control: ISM-0574; Revision: 7; Updated: Jun-23; Applicability: All; Essential Eight: N/A

SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).

Control: ISM-0861; Revision: 3; Updated: Sep-22; Applicability: All; Essential Eight: N/A

DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).

Control: ISM-1024; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Notifications of undeliverable emails are only sent to senders that can be verified via SPF or other trusted means.

Control: ISM-1872; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

Multi-factor authentication used for authenticating users of online services is phishing-resistant.

Control: ISM-1873; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML2

Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.

Control: ISM-1874; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML3

Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.

Control: ISM-1682; Revision: 3; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

Multi-factor authentication used for authenticating users of systems is phishing-resistant.

Control: ISM-1894; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML3

Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.

Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.

Ransomware Attacks

Ransomware attacks are a type of cyber-attack where malicious software (malware) encrypts a victim's data, rendering it inaccessible. The attacker then demands a ransom, typically in cryptocurrency, in exchange for a decryption key that can restore access to the data. Ransomware can spread through various methods, such as phishing emails, malicious attachments, or exploiting vulnerabilities in software.

These attacks can have severe consequences, including operational disruption, financial loss, and damage to an organisation's reputation. To defend against

ransomware, it is crucial to implement strong security measures, including regular data backups, restricting user access, maintaining up-to-date software, and educating users about the dangers of phishing and suspicious links. Having an incident response plan in place can help organisations quickly recover from an attack without paying the ransom.

Control: ISM-1511; Revision: 4; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.

Control: ISM-1810; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

Backups of data, applications and settings are synchronised to enable restoration to a common point in time.

Control: ISM-1811; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

Backups of data, applications and settings are retained in a secure and resilient manner.

Control: ISM-1812; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML1, ML2, ML3

Unprivileged accounts cannot access backups belonging to other accounts.

Control: ISM-1814; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML1, ML2, ML3

Unprivileged accounts are prevented from modifying and deleting backups.

Control: ISM-1707; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3

Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks are a type of cyber-attack aimed at overwhelming a targeted system, such as a website or network, with a flood of internet traffic. Unlike a traditional Denial of Service (DoS) attack, which typically originates from a single source, a DDoS attack involves multiple compromised computers or devices (often part of a botnet) working together to bombard the target with traffic. The goal of a DDoS attack is to exhaust the target's resources, such as bandwidth, processing power, or memory, rendering the service unavailable to legitimate users.

DDoS attacks can cause significant disruption to online services, leading to downtime, loss of revenue, and damage to an organisation's reputation. To mitigate DDoS attacks, organisations often use a combination of strategies, including deploying traffic filtering solutions, utilising Content Delivery Networks (CDNs) to distribute traffic, leveraging the infrastructure of cloud service providers, and implementing rate limiting to manage traffic flow. Having a well-prepared incident response plan is crucial for quickly identifying and responding to DDoS threats.

Control: ISM-1431; Revision: 5; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Denial-of-service attack mitigation strategies are discussed with cloud service providers, specifically:

- their capacity to withstand denial-of-service attacks
- costs likely to be incurred as a result of denial-of-service attacks
- availability monitoring and thresholds for notification of denial-of-service attacks
- thresholds for turning off any online services or functionality during denial-of-service attacks
- pre-approved actions that can be undertaken during denial-of-service attacks
- any arrangements with upstream service providers to block malicious network traffic as far upstream as possible.

Control: ISM-1436; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Critical online services are segregated from other online services that are more likely to be targeted as part of denial-of-service attacks.

Control: ISM-1437; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Cloud service providers are used for hosting online services.

Control: ISM-1438; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Where a high availability requirement exists for website hosting, CDNs that cache websites are used.

Control: ISM-1439; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

If using CDNs, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the CDNs and authorised management networks.

Control: ISM-1579; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.

Control: ISM-1580; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.

Control: ISM-1581; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Continuous real-time monitoring of the capacity and availability of online services is performed.

Control: ISM-1019; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A

A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.

Control: ISM-1805; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: N/A

A denial of service response plan for video conferencing and IP telephony services contains the following:

- how to identify signs of a denial-of-service attack
- how to identify the source of a denial-of-service attack
- how capabilities can be maintained during a denial-of-service attack
- what actions can be taken to respond to a denial-of-service attack.

Control: ISM-1335; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Wireless access points enable the use of the 802.11w amendment to protect management frames.

Control: ISM-1862; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A

If using a WAF, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the WAF and authorised management networks.

SQL Injection

SQL injection is a cyber-attack that targets databases by inserting malicious SQL code into an application's input fields, exploiting vulnerabilities where user input is improperly validated. This allows attackers to manipulate SQL queries, leading to potentially severe consequences such as unauthorised data access, data modification, or deletion. SQL injections can bypass authentication, compromise entire databases, and result in significant security breaches. To prevent SQL injections, it's important to validate and sanitise user inputs, use parameterised queries or prepared statements, and implement security measures to protect against such attacks.

Control: ISM-1240; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Validation or sanitisation is performed on all input handled by web applications.

Control: ISM-1270; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Database servers are placed on a different network segment to user workstations.

Control: ISM-1277; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Data communicated between database servers and web servers is encrypted.

Control: ISM-1275; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

All queries to databases from web applications are filtered for legitimate content and correct syntax.

Control: ISM-1276; Revision: 4; Updated: Dec-23; Applicability: All; Essential Eight: N/A

Parameterised queries or stored procedures, instead of dynamically generated queries, are used by web applications for database interactions.

Control: ISM-1278; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A

Web applications are designed or configured to provide as little error information as possible about the structure of databases.

Control: ISM-1536; Revision: 2; Updated: Dec-23; Applicability: All; Essential Eight: N/A

All queries to databases from web applications that are initiated by users, and any resulting crash or error messages, are centrally logged.

Rainbow Table

A rainbow table attack is a method used by attackers to crack hashed passwords by leveraging precomputed tables, known as rainbow tables, that map potential plaintext passwords to their corresponding hash values. When an attacker gains access to a hashed password, they can quickly compare it to the entries in a rainbow table to find the original password, making the attack much faster than traditional brute force methods. The efficiency of a rainbow table attack comes from the significant reduction in time required to crack a password, as the computationally intensive process of generating hash values is done beforehand.

To defend against rainbow table attacks, security practices such as salting are essential. A salt is a unique, random value added to each password before hashing, which ensures that even identical passwords produce different hashes. This makes it impractical to use rainbow tables, as the same table cannot be reused for multiple passwords. Using cryptographic hash functions that are computationally intensive, like bcrypt or Argon2, further slows down the process of generating and matching hashes, making it more difficult for attackers to succeed with rainbow table attacks.

Control: ISM-1402; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.

Control: ISM-1403; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.

Control: ISM-1749; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Cached credentials are limited to one previous logon.

Control: ISM-0418; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A

Credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.

Unpatched Software

Unpatched software vulnerabilities occur when flaws in software are not addressed by applying available updates or patches. These vulnerabilities can be exploited by attackers to gain unauthorised access, steal data, or disrupt operations. Since software vendors regularly release patches to fix known issues, failing to apply these updates leaves systems exposed to potential attacks, making unpatched vulnerabilities a common entry point for cyber criminals.

To mitigate the risks associated with unpatched software, organisations must implement a robust patch management process. This includes regularly monitoring for new patches, prioritising them based on the severity of the vulnerabilities, and applying them promptly across all systems. By staying proactive in patch management, organisations can significantly reduce the likelihood of being compromised by known vulnerabilities.

Control: ISM-1143; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A

Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.

Control: ISM-0298; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A

A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.

Control: ISM-1876; Revision: 0; Updated: Sep-23; Applicability: All; Essential Eight: ML1, ML2, ML3

Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1690; Revision: 2; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1700; Revision: 2; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Control: ISM-1701; Revision: 1; Updated: Sep-23; Applicability: All; Essential Eight: ML1, ML2, ML3

A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices

Control: ISM-1493; Revision: 5; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Software registers for workstations, servers, network devices and other IT equipment are developed, implemented, maintained and verified on a regular basis.

Control: ISM-1643; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A

Software registers contain versions and patch histories of applications, drivers, operating systems and firmware

Control: ISM-1903; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML3

Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Outdated Operating Systems

Outdated operating systems pose a significant security risk to organisations because they often lack the latest security patches and updates necessary to protect against known vulnerabilities. As operating systems age, vendors eventually stop providing support, leaving these systems exposed to new threats. Attackers can exploit these vulnerabilities to gain unauthorised access, disrupt services, or deploy malicious software. The longer an operating system remains outdated, the greater the risk, as attackers may specifically target these known weaknesses.

To mitigate the risks associated with outdated operating systems, organisations should prioritise upgrading to supported versions that receive regular security updates. Maintaining an inventory of all operating systems in use and conducting regular assessments to identify outdated systems is essential. By proactively managing and updating their operating systems, organisations can significantly reduce their exposure to potential exploits and enhance their overall security posture.

Control: ISM-1407; Revision: 5; Updated: Dec-22; Applicability: All; Essential Eight: ML3

The latest release, or the previous release, of operating systems are used.

Control: ISM-1501; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML1, ML2, ML3

Operating systems that are no longer supported by vendors are replaced.

Control: ISM-1809; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

When applications, operating systems, network devices or other IT equipment that are no longer supported by vendors cannot be immediately removed or replaced, compensating controls are implemented until such time that they can be removed or replaced.

Control: ISM-1409; Revision: 4; Updated: Dec-23; Applicability: All; Essential Eight: N/A

Operating systems are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-1695; Revision: 2; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2

Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.

Man-in-the-Middle (MitM) Attack:

Man-in-the-Middle (MitM) attacks are a form of cyber-attack where an attacker intercepts and potentially alters the communication between two parties without their knowledge. In a MitM attack, the attacker positions themselves between the victim and the intended recipient, such as between a user and a website, or between two communicating devices. The attacker can eavesdrop on the communication, steal sensitive information like login credentials or credit card numbers, and even alter the communication content to carry out further attacks.

MitM attacks can occur in various ways, including through unsecured Wi-Fi networks, compromised routers, or malicious software. The impact of such attacks can be severe, leading to unauthorised access to personal and corporate data, identity theft, and financial loss. To protect against MitM attacks, it is essential to use encryption protocols like HTTPS, secure VPNs, and strong authentication methods to ensure that communication is secure and cannot be easily intercepted or tampered with by unauthorised parties.

Control: ISM-0548; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Video conferencing and IP telephony calls are established using a secure session initiation protocol.

Control: ISM-0547; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Video conferencing and IP telephony calls are conducted using a secure real-time transport protocol.

Control: ISM-1139; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Only the latest version of TLS is used for TLS connections.

Control: ISM-1372; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

DH or ECDH is used for key establishment of TLS connections.

Control: ISM-1453; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Perfect Forward Secrecy (PFS) is used for TLS connections.

Control: ISM-0554; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Control: ISM-1373; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Anonymous DH is not used for TLS connections.

Control: ISM-0485; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Public key-based authentication is used for SSH connections.

Control: ISM-1374; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

SHA-2-based certificates are used for TLS connections.

Control: ISM-0484; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A

The SSH daemon is configured to:

- only listen on the required interfaces (ListenAddress xxx.xxx.xxx.xxx)
- have a suitable login banner (Banner x)
- have a login authentication timeout of no more than 60 seconds (LoginGraceTime 60)
- disable host-based authentication (HostbasedAuthentication no)
- disable rhosts-based authentication (IgnoreRhosts yes)
- disable the ability to login directly as root (PermitRootLogin no)
- disable empty passwords (PermitEmptyPasswords no)
- disable connection forwarding (AllowTCPForwarding no)

- disable gateway ports (GatewayPorts no)
- disable X11 forwarding (X11Forwarding no).

Insider Threats

Insider threats refer to the risks that originate from individuals within an organisation who have authorised access to its systems, data, or networks. These individuals, whether employees, contractors, or business partners, can intentionally or unintentionally misuse their access to cause harm. Insider threats are particularly challenging to detect because insiders already possess legitimate access, making their malicious activities less apparent compared to external threats. They can lead to severe consequences, including data breaches, financial loss, and damage to an organisation's reputation.

These threats can manifest in various forms, such as data theft, sabotage, or the unauthorised sharing of sensitive information. Insiders may act out of financial gain, personal grievances, or coercion by external entities, while unintentional insider threats might occur due to negligence, lack of awareness, or human error. Given the complexity and potential impact of insider threats, organisations must implement security measures, including continuous monitoring, strict access controls, and comprehensive insider threat mitigation programs, to detect and prevent such incidents effectively.

Control: ISM-1625; Revision: 2; Updated: Jun-24; Applicability: All; Essential Eight: N/A

An insider threat mitigation program is developed, implemented and maintained.

Control: ISM-1626; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Legal advice is sought regarding the development and implementation of an insider threat mitigation program.

Control: ISM-1073; Revision: 6; Updated: Jun-24; Applicability: All; Essential Eight: N/A

An organisation's systems, applications and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Control: ISM-1576; Revision: 3; Updated: Jun-24; Applicability: All; Essential Eight: N/A

If an organisation's systems, applications or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.

Control: ISM-0585; Revision: 6; Updated: Jun-24; Applicability: All; Essential Eight: N/A

For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the information technology equipment involved are recorded.

Control: ISM-0109; Revision: 9; Updated: Dec-23; Applicability: All; Essential Eight: ML3

Event logs from workstations are analysed in a timely manner to detect cyber security events.

Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: ML2, ML3

Cyber security events are analysed in a timely manner to identify cyber security incidents.

Control: ISM-0120; Revision: 5; Updated: May-20; Applicability: All; Essential Eight: N/A

Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Control: ISM-0735; Revision: 3; Updated: Dec-22; Applicability: All; Essential Eight: N/A

The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.

Control: ISM-1634; Revision: 1; Updated: Jun-22; Applicability: All; Essential Eight: N/A

System owners select controls for each system and tailor them to achieve desired security objectives.

Control: ISM-0720; Revision: 3; Updated: Sep-23; Applicability: All; Essential Eight: N/A

The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.

Control: ISM-1073; Revision: 6; Updated: Jun-24; Applicability: All; Essential Eight: N/A

An organisation’s systems, applications and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Change Log

Date	Changes/Event
26 August 2024	Published v.1

Contact

For any feedback or comments, please reach out to Eimear Leyne on LinkedIn