**DLUHC-CS-P001 ITHC Principle Security Concerns**

**Prepared by the Department for Levelling Up, Housing & Communities**

**Date: March 2022**

**Version: v1.0**

The information contained in this document is restricted as per the protective marking, and only for the information of the intended recipient(s) and may not be used, published or redistributed without the prior consent of MHCLG. The opinions expressed are in good faith and while every care has been taken in preparing this document, MHCLG makes no representations of whatever nature in respect of this document

Contents

**Introduction 3**

Purpose 3

Scope 3

Principle Security Concerns **4**

Backup 4

Multi-factor Authentication 4

Operating Systems 5

Active Directory 6

Logging 6

OWASP Application Top 10 categories 7

OWASP API Security Top 10 8

Firewall Configurations 9

Network Configurations (switches, routers and wireless access points) 9

1. Introduction
   1. Purpose

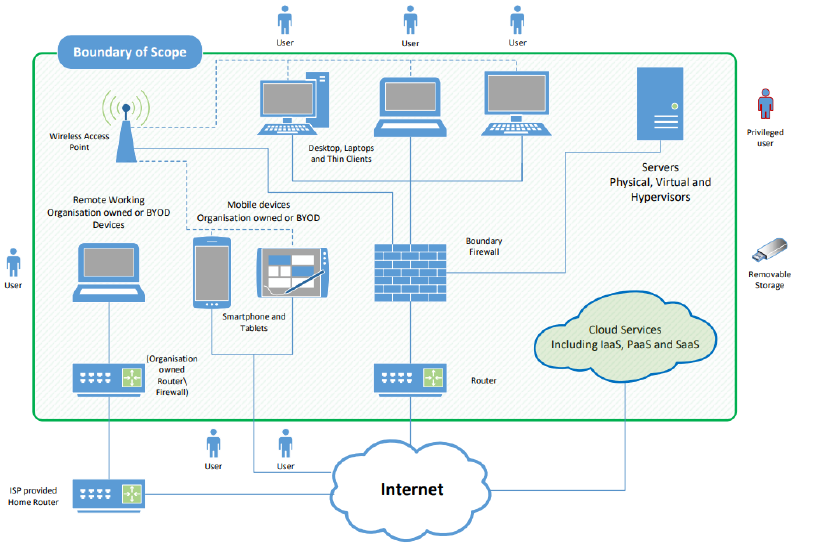
This document presents a categorised set of Principle Security Concerns (PSC) for use within an IT

Health Check (ITHC) scoping document. The PSCs have been derived following a recent Department for Levelling Up, Housing & Communities (DLUHC) and National Cyber Security Centre (NCSC) ‘Mitigating Malware and Ransomware’ survey being conducted with Local Authorities during 2021/2022. The suite of PSCs will assist Local Authorities to generate penetration testing scopes aligned with NCSC areas of concerns and pertinent cyber threats.

* 1. Scope

The PSCs are categorised into 9 focus areas identified below as those providing defences against ransomware and malware threats, viewed from an identify, protect, detect, respond and recover perspective.[[1]](#footnote-1)​ Focus areas in scope are:

* Backup
* Multi-factor Authentication
* Operating Systems
* Active Directory
* Logging
* OWASP Application Top 10
* OWASP API Security Top 10
* Firewall Configurations
* Network Configurations (switches, routers and wireless access points)



1. Principle Security Concerns
   1. Backup

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-BU1 | Active Directory should be backed up as it severely limits the Council’s ability to recover AD services. |
| PSC-BU2 | Backup traffic and data must be encrypted using approved strong encryption algorithms and not be communicated in cleartext protocols. Backups should be stored encrypted otherwise potentially exposing confidential and sensitive information. |
| PSC-BU3 | Backup copies have ‘air-gap’ between the backup mechanism and the copies of the data. |
| PSC-BU4 | Backup service accounts should not utilise weak and or non-complex password(s). Credentials should not be locally cached on the backup servers(s). |
| PSC-BU5 | Backup servers must not expose SMB service as this increases the attack surface for ransomware propagation. |
| PSC-BU6 | Administration of backup servers via remote desktop protocol should be restricted from within the local area network. |

* 1. Multi-factor Authentication

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-MFA01 | Cloud based administration accounts aren’t protected with MFA exposing potential attack areas. |
| PSC-MFA02 | External remote access is provided via single factor authentication only. |
| PSC-MFA03 | On-premise privileged user account access is provided via single factor authentication only. |
| PSC-MFA04 | Mobile devices should be controlled using an MDM service to enforce technical controls. |
| PSC-MFA05 | Dependent on the devices you are provisioning in your IT estate, you should use an Enterprise Mobility Management (EMM) that supports OEMConfig. |
| PSC-MFA06 | Configure the logging and monitoring capabilities of the MDM. |
| PSC-MFA07 | If a Virtual Private Network (VPN) is required, you should use a third-party application. |
| PSC-MFA08 | Third-party apps for work use (“managed apps”) should be approved centrally into an enterprise application catalogue. Either automatically install them during setup or make them available in the Managed Google Play Store or Apple Business Manager. |
| PSC-MFA09 | Consider your approach to enabling enterprise-owned Google accounts on users’ devices, using on-device policies to manage specific Google features. |
| PSC-MFA10 | Antivirus and other security software are not recommended on Android or Apple mobile devices. |

* 1. Operating Systems

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-OS1 | Unsupported operating systems are present within the estate with known vulnerabilities and/or have access to untrusted internet content. |
| PSC-OS2 | Supported operating systems are not patched within 14 days of vendor release. |
| PSC-OS3 | Vulnerable systems have exposed services which may provide a mechanism for an attacker to gain a foothold. |
| PSC-OS4 | Antivirus / antimalware software is not present on target systems, increasing likelihood of successful malicious software insertion. |
| PSC-OS5 | Cached administrator credentials are present on systems increasing likelihood of successful privilege escalation attacks. |
| PSC-OS6 | All servers (not limited to domain controllers and backup servers), EUDs and the operating systems are not hardened in line with best practice – Centre for Internet Security (CIS) Level 2 |
| PSC-OS7 | Application whitelisting should be in place across critical systems to prevent known malicious code from executing. |
| PSC-OS8 | Host based firewalls are not present and provide an increased attack surface or Host-based firewall rulesets are overly permissive providing little efficacy in filtering non-essential traffic. |
| PSC-OS9 | Mobile and tablet operating systems are not running a vendor supported release in receipt of security updates and/or are not secured in accordance with NCSC guidance. |

* 1. Active Directory

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-AD1 | Coarse grained privileged user account permissions provide a large account base with logon privileges to domain controllers. |
| PSC-AD2 | User accounts and accounts with domain wide permissions must specify minimum password lengths for each, adopting the 'three random words' technique can help users to use suitably complex passphrases that they can actually remember. |
| PSC-AD3 | Password systems to be configured so that there is a progressively increasing time delay between successive login attempts - This restricts the number of guesses an attacker can attempt while giving users multiple opportunities to remember their password |

* 1. Logging

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-LOG1 | Privileged user account logon success / failure should be centrally logged and alerted upon. |
| PSC-LOG2 | User MFA authentication failures should be logged / alerted upon. |
| PSC-LOG3 | Cloud service logs should not be isolated and ingested into a central system for analysis and alerting. |
| PSC-LOG4 | Alerting to be configured within the central logging / SIEM solution to trigger event investigation and triage. |
| PSC-LOG5 | Event correlation rules configured so that alerting and detection of potential nefarious activity is reported and investigated. |
| PSC-LOG6 | Logs must not be susceptible to compromise / tampering as a consequence of weak RBAC controls. |
| PSC-LOG7 | Log retention is be kept for 6 months otherwise limiting historical analysis and investigative capability. |

* 1. OWASP Application Top 10

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC- OWASP1 | Broken Access Control- Each piece of information should be available only to a specific set of users based on the access they have been granted. Broken access control may lead to scenarios where users can access the information they don't have the authority to access. |
| PSC- OWASP2 | Cryptographic Failures- Focus on failures related to cryptography. Rather than directly attacking a system, hackers often try to steal data while it is in transit from the user's browser. |
| PSC- OWASP3 | Injection- When the attacker pollutes the query sent to the back-end application with a valid code that is executed by the end target, hackers can gain access to protected data or even execute OS commands. |
| PSC- OWASP4 | Insecure Design- Refers to a design without threat modelling, secure design patterns and principles, and reference architectures. |
| PSC- OWASP5 | Security Misconfiguration- These can be in the form of unnecessary open ports, default accounts and passwords, mishandling errors that reveal too much information about the application. |
| PSC- OWASP6 | Vulnerable and Outdated Components ensure that you identify vulnerable and outdated components. |
| PSC- OWASP7 | Identification and Authentication Failures- Weakness in place if applications permit credential stuffing, brute force or other nominated attacks, default or weak passwords, uses plain text, missing or ineffective MFA to name some. |
| PSC- OWASP8 | Software Logging and Monitoring Failures- Relates to code and infrastructure that does not protect against integrity violations. Many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. |
| PSC- OWASP9 | Security Logging and Monitoring Failure- Help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. |
| PSC- OWASP10 | Server-Side Request Forgery (SSRF)- Whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL). |

* 1. OWASP API Security Top 10

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-API1 | Broken Object Level Authorisation- APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorisation checks should be considered in every function that accesses a data source using an input from the user. |
| PSC-API2 | Broken User Authentication- Allows attackers to compromise authentication tokens or to exploit implementation flaws to assume other user’s identities temporarily or permanently. Compromising a system’s ability to identify the client/user, compromises API security overall. |
| PSC-API3 | Excessive Data Exposure- Expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user. |
| PSC-API4 | Lack of Resources & Rate Limiting- Some APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force. |
| PSC-API5 | Broken Function Level Authorisation- Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorisation flaws. By exploiting these issues, attackers gain access to other users’ resources and/or administrative functions. |
| PSC-API6 | Mass Assignment- Binding client provided data to data models, without proper properties filtering based on an allow list, usually leads to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to. |
| PSC-API7 | Security Misconfiguration- Unsecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information. |
| PSC-API8 | Injection- Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorisation. |
| PSC-API9 | Improper Asset Management expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints. |
| PSC-API10 | Insufficient Logging and Monitoring- Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. |

* 1. Firewall Configurations

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC- FWC1 | Change any default administrative password to an alternative that is  difficult to guess (see password-based authentication) — or disable remote  administrative access entirely. |
| PSC- FWC2 | Prevent access to the administrative interface (used to manage firewall  configuration) from the internet, unless there is a clear and documented  business need and the interface is protected by one of the following  controls:   * multi-factor authentication (see MFA details below) * an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach |
| PSC- FWC3 | Block unauthenticated inbound connections by default. |
| PSC- FWC4 | Ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation. |
| PSC- FWC5 | Remove or disable unnecessary firewall rules quickly, when they are no longer needed. |
| PSC- FWC6 | Use a software firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots. |

* 1. Network Configurations (switches, routers and wireless access points)

|  |  |
| --- | --- |
| **PSC ID** | **Description** |
| PSC-API1 | Remove and disable unnecessary user accounts (such as guest accounts  and administrative accounts that won’t be used). |
| PSC-API2 | Change any default or guessable account passwords. |
| PSC-API3 | Remove or disable unnecessary software (including applications, system utilities and network services). |
| PSC-API4 | Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the internet). |
| PSC-API5 | Ensure authentication of users before allowing access to organisational data or services. |
| PSC-API6 | Ensure appropriate device locking controls for physically present users. Users must unlock devices using credentials such as biometric, password or pin before gaining access to any services. |
| PSC-API7 | Use standardised security configurations for the WLAN components, such as client devices and APIs. |
| PSC-API8 | Separate WLANs with different security profiles. For example, there should be separate WLANs for external users, e.g. guests and internal users. Devices on a Council’s external WLAN should not be able to connect through the WLAN to devices on another of the Council’s WLANs. This helps to protect the  Council’s other networks and devices from external devices and users. |
| PSC-API9 | For external WLANs that do need internal network access, WLAN client devices should be allowed access only to the necessary hosts or subnets using only the required protocols. |
| PSC-API10 | For all their WLAN client devices: disable all network interfaces that are not authorised for any use and configure the device so that the user cannot enable them or otherwise circumvent the restrictions. |
| PSC-API11 | Configure host-based network security tools (e.g., host-based firewalls, host-based intrusion detection and prevention systems) to prevent multiple network interfaces from being used at one time. |
| PSC-API12 | Enable specialised software-based controls that permit either WLAN or wired network access, but not both simultaneously. These controls could be built into the Operating System (OS). |
| PSC-API13 | Specify and enforce authorised network profiles and/or unauthorized profiles through OS/domain controls, third party policy-based software. |

1. IT Health Check and NCSC ACD excluded. [↑](#footnote-ref-1)