LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

MHCLG-CS-P001 ITHC Principle Security Concerns

Prepared by the Ministry of Housing, Communities and Local Government (MHCLG)

Date: 15th March 2021

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

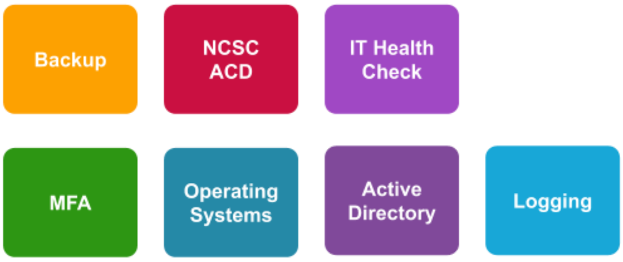
1 Introduction

1.1 Purpose

This document presents a categorised set of Principle Security Concerns (PSC) for use within an IT Health Check scoping document. The PSCs have been derived following a recent Ministry of Housing, Communities and Local Government (MHCLG) Mitigating Malware and Ransomware Survey conducted with Local Authorities during 2020. The suite of PSCs will assist Local Authorities to generate penetration testing scopes aligned with National Cyber Security Centre (NCSC) areas of concerns and pertinent cyber threats.

1.2 Scope

The PSCs are categorised into focus areas identified below as those providing defenses against ransomware and malware threats, viewed from an identify, protect, detect, respond and recover perspective.[1]



[1] IT Health Check and NCSC ACD excluded.

2 Principle Security Concerns

2.1 Backup

PSC ID	Description
PSC-BU1	Organisations Active Directory system state is not being backed up and severely limits the organisation’s ability to recover directory services.
PSC-BU2	Backup traffic is communicated in cleartext protocols and sensitive information is vulnerable to eavesdropping.
PSC-BU3	Backup traffic is channel encrypted which allows sub optimal cipher suites.
PSC-BU4	Backups are stored unencrypted potentially exposing sensitive information.
PSC-BU5	Backups are stored using a weak encryption algorithm affording poor confidentiality protection.
PSC-BU6	Backup servers are not leveraging latest build releases which may introduce known vulnerabilities.
PSC-BU7	Backup servers are sub-optimally configured exposing unused services.
PSC-BU8	Backup server operating systems are not hardened in line with best practice – Centre for Internet Security (CIS) Level 2
PSC-BU9	Backup servers reside within the corporate Active Directory domain providing no defence against an escalated privilege lateral attack.
PSC-BU10	Backups are stored on-network within the same authentication domain.
PSC-BU11	Backup service accounts utilise weak and or non-complex password(s).

PSC-BU12	Backup service account(s) credentials are locally cached on the backup server(s).
PSC-BU13	Backup servers expose SMB service, increasing the attack surface for ransomware propagation.
PSC-BU14	Administration of backup servers via remote desktop protocol is unrestricted from within the local area network.

2.2 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 leveraging user based authentication is only a single factor.
PSC-MFA03	On-premise privileged user account access is provided via single factor authentication only.

2.3 Operating Systems

PSC ID	**Description**
PSC-OS1	Unsupported operating systems are present within the estate with known vulnerabilities.
PSC-OS2	Supported operating systems are not patched within 14 days of vendor release.

PSC-OS3	Unsupported systems have access to untrusted internet content.
PSC-OS4	Vulnerable systems have exposed services which may provide a mechanism for an attacker to gain a foothold.
PSC-OS5	Host based firewalls are not present and provide an increased attack surface.
PSC-OS6	Antivirus / antimalware software is not present on target systems, increasing likelihood of successful malicious software insertion.
PSC-OS7	Cached administrator credentials are present on systems increasing likelihood of successful privilege escalation attacks.
PSC-OS8	Desktop operating systems are not hardened in line with best practice – Centre for Internet Security (CIS) Level 2.
PSC-OS9	Application whitelisting is not in place across critical systems to prevent known malicious code from executing.
PSC-OS10	Host-based firewall rulesets are overly permissive providing little efficacy in filtering non-essential traffic.
PSC-OS11	Mobile and tablet operating systems are not running a vendor supported release in receipt of security updates.
PSC-OS12	Mobile devices are not subject to mobile device management technical governance.
PSC-OS13	Mobile devices are not secured in accordance with NCSC guidance.

PSC-OS14	Server operating systems are not hardened in line with best practice – Centre for Internet Security (CIS) Level 2.

2.4 Active Directory

PSC ID	**Description**
PSC-AD1	Domain controllers are insufficiently hardened in accordance with industry best practice (CIS benchmark level 2) .
PSC-AD2	Coarse grained privileged user account permissions provide a large account base with logon privileges to domain controllers.
PSC-AD3	Complex passwords are not in place for privileged user accounts with domain wide permissions.
PSC-AD4	Local administrator accounts may be standardised throughout server estate and therefore more susceptible to attack upon one being compromised.
PSC-AD5	Standard user accounts are utilising passwords susceptible to brute force attacks.
PSC-AD6	Accounts are susceptible to continuous login attempts with throttling / lockout controls being absent.

2.5 Logging

PSC ID	**Description**
PSC-LOG1	Privileged user account logon success / failure is not centrally logged and alerted upon.

PSC-LOG2	User MFA authentication failures are not logged / alerted upon, resulting in nefarious activity potentially going undetected.
PSC-LOG3	Cloud service logs are isolated and not ingested into a central system for analysis and alerting.
PSC-LOG4	No alerting is configured within the central logging / SIEM solution to trigger event investigation and triage.
PSC-LOG5	Lack of event correlation rules limit alerting and detection of potential nefarious activity.
PSC-LOG6	Logs are susceptible to compromise / tampering as a consequence of weak RBAC controls
PSC-LOG7	Log retention is less than 6 months potentially limiting historical analysis and investigative capability.
PSC-LOG8	Backup job success / failure is not centrally logged and alerted upon.