LOCAL DIGITAL Cyber

Ministry of Housing, Communities & Local Government

East Hampshire District Council

Cyber Treatment Plan

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

Date: 30th March 2021

Version: v1.0

Contents

Use the links below to jump to a section of this report.

Document Control

Title	East Hampshire District Council Cyber Treatment Plan
Reference	MHCLG-CS-CTP-132-South Gloucestershire
Prepared By	Ministry of Housing, Communities and Local Government
Date	30th March 2021
Version	1.0

Distribution

Name	Title	Organisation
Susan Parker	Head of Service	Havant Borough Council

Overview

The cyber treatment plan shows, for each remediation finding, a desired timeline in which it's recommended to remediate and treat each finding.

Cyber Support Functions

Areas of support	
Cyber treatment planning	In line with business priorities, a guided session to output a cyber treatment plan structured around report findings to address cyber remediation actions.
NCSC Active Cyber Defence	Assistance for ACD service on-boarding and hands-on deployment of Logging Made Easy.
Infrastructure configuration/support	Supported ‘hands-on’ to assist with configuration and/or patching verification, GPO configuration test/deployment
Design Review and guidance for technical enhancement	Review of current technical offering to address a remediation with enhanced design. Guidance is also available if a new solution is to be progressed.
Tooling support	Cyber Support tooling (deployment of) to assist with wider and longer term cyber protection
ITHC PSC	Guidance and review of current ITHC PSC, with a view to aligning PSC so to target ransomware threat
RTO/RPO Strategy	Guidance for best practice so to determine an RTO (Return to Operation) and RPO (Recovery Point Objective) for recovery

Timeline and Expectations

Timeline set in fiscal year e.g. Q4 ends 31st March 2021. Q1 starts 1st April 2021.

Cyber Rating/Area	Timeline expectations
Backup (all ratings)	Commence Q1 2021 and to target delivery no later than end of Q2 2021
NCSC Active Cyber Defence (all ratings)	Aim to complete within Q1 2021
High	Commence Q1 2021 and to target delivery no later than end of Q2 2021
Medium rating	Target completion Q2 2021/Q3 2021
Low rating	Target completion Q3/Q4 2021

Cyber Treatment Plan

Cyber Treatment Plan						2021					
Rec	**Area**	**Topic**	**Recommendation**	**Rating**		**Q4**	**Q1**	**Q2**	**Q3**	**Cyber Support**	**Comments**
R1	Backup	BK1	Offline backup media should be implemented in addition to the current utilised configuration to give an ‘air-gap’ between the backup mechanism and the copies of the data. This can either be a tape based system or removable media drives which are then securely stored.	High						Design Support	Technical session with MHCLG to support backup design enhancement.
R2	Backup	BK2	Formalised backup regime with appropriately detailed backup documentation.	Medium						N/A	
R3	Backup	BK2	Creation of recovery work instructions providing clear step-by-step recovery procedural guidance.	Medium						N/A	
R4	Backup	BK3	Implementation of a 3rd party solution to deliver data backup of the online services.	High						Design Support	Technical session with MHCLG to support backup

											design enhancement.
R5	Backup	BK4	Implementation of a 3rd party solution to deliver data backup of the online email services.	High						Design Support	Technical session with MHCLG to support backup design enhancement.
R6	Backup	BK4	Define and implement retention policies for all email data.	Low						N/A	
R7	Backup	BK5	TX logs and Journaling files should be backed up more frequently than once per day in order to provide a better recovery point than within the current 24 hours for all systems. The criticality of each system should be reviewed in order to set the precise frequency of these backups. I.e. critical systems ideally should have TX logs backed up every 15 minutes (but hourly would be a good compromise), whilst low priority systems can be set to every 1 or 2 hours (but again once a day at midday would reduce the RPO by 50% in one go). These should be agreed with	Medium						MHCLG Artefact	Share TCX Log with council

			the system owners and documented. The Oracle Systems should also have their backup regime documented fully.								
R8	Backup	BK5	Backup recovery capability should be signed off by the system owners.	Medium						N/A	
R9	Backup	BK6	Document the access to the Veritas Console, and the recovery procedures.	Low						N/A	
R10	Backup	BK8	Following the individual system failover test in March carry out a full BC/DR test as soon as possible.	Medium						N/A	
R11	MFA	MFA1	Once M365 rollout is complete, plan and remove the existing VPN solution in order to remove a potential ‘backdoor’ access route into the council estate	Low						N/A	
R12	MFA	MFA2	Extend the MFA to secure logins to the Active Directory for privileged access roles including management of Backups.	Medium						N/A	
R13	AD	AD1	Document the RBAC / Least Privilege model	Low						N/A	
R14	AD	AD1	Audit the privileged roles on a regular basis.	Low						N/A	
R15	AD	AD3	Review password policies, ensuring alignment with current NCSC guidance.	Medium						N/A	
R16	AD	AD5	Implement a geographically diverse Domain Controller for the shared domain into the secondary Data Centre.	Low						N/A	

R17	ACD	ACD1	Onboard all external IP addresses onto NCSC EWS.	Medium						N/A	
R18	ACD	ACD2	Confirm that all council websites (local and publicly hosted) are onboarded into Web Check.	Medium						N/A	
R19	ACD	ACD2	Confirm that all locally hosted websites have no external visibility	Medium						N/A	
R20	ACD	ACD3	Implement Protective DNS	Medium						NCSC ACD	MHCLG Team to support onboarding
R21	ACD	ACD4	Onboard email service onto Active Cyber Defence Mail Check	High						NCSC Support	Support session with NCSC MailCheck Lead
R22	ACD	ACD4	Ensure DMARC policy is set to “Reject”	Low						NCSC Support	Support session with NCSC MailCheck Lead
R23	ACD	ACD4	Configure Forensic reports and ensure they are sent to a central mailbox for post incident analysis.	Low						N/A	
R24	ACD	ACD6	Sign up to, plan and carry out EiaB exercises as soon as practicable.	Medium						N/A	

R25	OS	OS1	Tighten up the GPO's to secure the Windows servers without incurring operational faults.	Medium						N/A	
R26	OS	OS2	Complete the in progress migration strategy to remove all unsupported Operating Systems (from the environment and to migrate to the highest available supported level of Operating Systems (from the application perspective), or move them to Azure Public which will allow for a slightly longer operational lifespan whilst they are migrated off 2008R2.	Medium						N/A	
R27	HC	HC2	Widen ITHC scope to incorporate key council security enforcement controls and non-PSN systems.	Medium						ITHC Support	ITHC Session
R28	HC	HC3	Define council Principle Security Concerns for inclusion within ITHC scope documentation.	Low						ITHC Support	PSC session
R29	HC	HC5	Implement a Vulnerability Scanning solution and then carry out a schedule of regular, planned authenticated vulnerability scanning across the enterprise.	Medium						Tooling Support	MHCLG OpenVas demo

MHCLG Support Activities

Rec	Area	Topic	Recommendation	Rating		Cyber Support	Comments
R1	Backup	BK1	Offline backup media should be implemented in addition to the current utilised configuration to give an 'air-gap' between the backup mechanism and the copies of the data. This can either be a tape based system or removable media drives which are then securely stored.	High		Design Support	Technical session with MHCLG to support backup design enhancement.
R4	Backup	BK3	Implementation of a 3rd party solution to deliver data backup of the online services.	High		Design Support	Technical session with MHCLG to support backup design enhancement.
R5	Backup	BK4	Implementation of a 3rd party solution to deliver data backup of the online email services.	High		Design Support	Technical session with MHCLG to support backup design enhancement.

R20	ACD	ACD3	Implement Protective DNS	Medium		NCSC ACD	MHCLG Team to support onboarding
R21	ACD	ACD4	Onboard email service onto Active Cyber Defence Mail Check	High		NCSC Support	Support session with NCSC MailCheck Lead
R22	ACD	ACD4	Ensure DMARC policy is set to “Reject”	Low		NCSC Support	Support session with NCSC MailCheck Lead
R27	HC	HC2	Widen ITHC scope to incorporate key council security enforcement controls and non-PSN systems.	Medium		ITHC Support	ITHC Session

R28	HC	HC3	Define council Principle Security Concerns for inclusion within ITHC scope documentation.	Low	ITHC Support	PSC session
R29	HC	HC5	Implement a Vulnerability Scanning solution and then carry out a schedule of regular, planned authenticated vulnerability scanning across the enterprise.	Medium	Tooling Support	MHCLG OpenVas demo