Overview of MFA best practice

V1.2

Objective

Outline guidance and approach to best practice design features for the use of Multi Factor Authentication (MFA) options for use within Local Authority Information Systems.

MFA helps prevent attackers from accessing your systems even if they obtain your username and password.
For example, if you create a multi-layered mechanism, an unauthorised user would have to defeat all layers to gain access

How does Multi Factor Authentication work ?

Multi Factor Authentication works on the principle of requiring <u>at least two</u> of these items:

- Something you have (such an authentication application on your phone)
- Something you know (such as your username and password)
- Something you are (such as fingerprint or iris recognition)

For remote system access, MFA is usually built up of the first two items, but the authentication applications can also require the third item.

LOCAL DIGITAL Cyber

Best practices

Best practices for the usage of MFA are :

- Protection of Online Administrative Accounts (Such as M365 Global Administrators)

- Protection of Internal Domain Privileged Accounts (Such as Domain Administrators, SAN Administrators, Backup Server Accounts)

- Protection of User Accounts for Remote Access

- Protection of Regular M365 User Accounts when not in 'Whitelisted' locations

LOCAL DIGITAL | Cyber

Best practices (cont.)

Best practices for the usage of MFA are:

- NCSC Guidance on MFA explicitly states that "All users, including administrators, should use multi-factor authentication when:

    - using Cloud and Internet-connected services.

    - authenticating to services that hold sensitive or private data.

- Administrators should, wherever possible, be required to use multi-factor authentication."

- Councils should therefore consider carefully the use of services which only allow for single-factor authentication.

LOCAL DIGITAL | Cyber

Why are these practices important?

Using MFA for VPN Remote Access:

- Stops unauthorised access if a stolen username and password is used.
  A VPN is, after all, a direct link into your Council's network.

Using MFA on M365 Global Administrator Accounts:

- A M365 Global Administrator Account is an incredibly important account, and if compromised you can find yourself locked out of your entire infrastructure, or an attacker could readily carry out a range of malicious actions. It should be treated as 'The Keys to the Kingdom' and protected with an extremely secure password, and **at least** one other form of Authentication.

LOCAL DIGITAL | Cyber

Why are these practices important? (cont.)

Using MFA on On Premise Privileged User Accounts:

- These accounts are extremely important and unauthorised usage can result in significant damage to internal systems. As with other items listed, requiring additional authentication will help protect the accounts even if a valid username and password are used to access key services such as Domain Controllers, Storage Systems, etc.

Using MFA on M365 User Accounts when not onsite:

- By using a specific type of Conditional Access Policy you can require a user to use MFA when accessing their emails or Microsoft 365 located files when they are not connected to your local network, or trusted locations. This will reduce user impact by allowing them to connect with just usernames and passwords when working internally.

LOCAL DIGITAL | Cyber

How to implement MFA

- For Microsoft 365 Accounts the most common implementation model is to use the Microsoft Authenticator App on a user's Mobile Device.
    - This application is free to use, and is designed to be integrated with M365

- For On Premise Domain accounts (privileged or not) you can use any number of MFA systems; some are free, others are chargeable. Suitability should be assessed before selecting one.
    - Options include but are not limited to Microsoft Authenticator App, Google Authenticator App, Cisco Duo, RSA.

- For standalone systems, check with the system manufacturer for compatibility as not all manufacturers currently support MFA. Support for MFA should be a consideration when procuring a new system

LOCAL DIGITAL | Cyber

How to implement MFA (cont.)

- Overview:
  https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authentication

- On Premise Options (No Integration with Azure AD)
  - ManageEngine ADSelfService Plus:
    https://www.manageengine.com/products/self-service-password/windows-logon-two-factor-authentication.html?lhs
  - Cisco Duo:
    https://duo.com/blog/protecting-windows-servers-and-remote-desktops-with-duo

- Where Active Directory is Integrated into Azure AD (M365):
  - Azure MFA
    https://docs.microsoft.com/en-GB/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

LOCAL DIGITAL Cyber

Jump Servers, RBAC Integration & MFA

- Consider the use of Jump Servers with the relevant administration tools on them (eg. Active Directory Management, SQL Management, Exchange Management, etc) as the servers to implement MFA onto.

- Your privileged users should use their MFA enabled privileged accounts to log onto these servers to carry out the administrative tasks, rather than going to the servers directly.

LOCAL DIGITAL | Cyber

Final considerations:*

- You will need to consider how administrators can gain access to the service if multi-factor authentication is unavailable. This could be caused by a service configuration or the loss of an authentication token.

- Creating an emergency ('break glass') account would give you the capability to log into a server which has administrative accounts protected by MFA in the event of an MFA service failure. These accounts should have hyper-complex passwords and known only to a small number of high level administrators, ideally in a Password 'Safe' product, so the passwords are not easily viewed.

- Accounts such as an emergency or 'break glass' accounts that use a single authentication factor should be the subject of increased protective monitoring so that any misuse can be easily detected.

* https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

LOCAL DIGITAL | Cyber

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book using this link: https://calendly.com/andrea-baron/ad-hoc-call-with-council .
These are longer 1:1 sessions between DLUHC cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber support drop in sessions every Wednesday for 30 minute session between 2pm - 4pm. These regular 1:1 sessions are available for you to book anytime using the Calendly link: https://calendly.com/andrea-baron/drop-in-support-session .

Cyber clinics are occurring on the 3rd Thursday of the month between 11.30am - 12.30pm where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

LOCAL DIGITAL | Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on [Medium](#)
- Follow LDCU on Twitter ([@LDgovUK](#))
- Subscribe to our [Cyber newsletter](#) for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC [Digital blog](#)

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email [cybersupport@localdigital.gov.uk](#).

LOCAL DIGITAL | Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

🐦 **@LDgovUK**

www.localdigital.gov.uk

#LocalDigital   #FixThePlumbing

LOCAL DIGITAL Cyber