Solution Brief

BROADCOM
MAINFRAME SOFTWARE

Phishing Resilience on the Mainframe

Best Practices for Safeguarding Your Credentials with Advanced Authentication Mainframe, Trusted Access Manager for Z, and Cleanup

Overview

Like any other platform, the mainframe is susceptible to cyberattacks. Nefarious practices like phishing are on the rise, and your mainframe could be a target. Phishing is a type of cyberattack in which an attacker sends a fraudulent email with the aim of inducing its recipients to reveal sensitive information, such as user credentials, or to deploy malicious software, such as ransomware.

A user's ID and password control mainframe access. If a user falls victim to a phishing attack that compromises their mainframe credentials, the attacker now has access to your mainframe.

To mitigate the risks of cyberattacks such as phishing, follow these best practices for safeguarding mainframe credentials:

- Use multi-factor authentication on critical applications, groups or accounts, especially those that can affect systems or critical applications (Advanced Authentication Mainframe).
- Manage users with highest privileges using a privileged access management solution (Trusted Access Manager for Z).
- Clean up the security database to reduce exposure from over-provisioned accounts (Cleanup).

Let us review each of these best practices and explore how Broadcom® security solutions can help.

Use Multi-factor Authentication on Critical Accounts

Successful phishing results in the loss of control of IDs and passwords that can be used to access critical systems and applications. Adding multi-factor authentication to a system means users must provide additional pieces of evidence to verify their identity before they can access the mainframe.

By employing another factor, phishing is significantly more difficult for the perpetrator. The mainframe's resilience to phishing attacks is increased.

Advanced Authentication Mainframe from Broadcom lets users log in to mainframe applications using multi-factor authentication credentials. Advanced Authentication Mainframe enables granular deployment allowing for use with specific applications, users, or even roles—eliminating an *all or nothing* approach.

Through increased diligence in verifying the identity of users who seek access to the mainframe, Advanced Authentication Mainframe helps you prevent data breaches such as those caused by phishing and other cyberattacks.

Manage Privileged Users with a Privileged Access Management Solution

Management of any system requires certain users to hold privileged entitlements that enable them to make necessary changes to critical systems and applications. These same credentials, in the wrong hands, could result in catastrophic loss of data and systems.

A best practice is to manage these users and restrict their use of privileged entitlements to an *as needed* basis. By providing an entitlement only when needed, the result is an ID that is not entitled most of the time. Should theft of the credentials occur, the risky entitlements associated are not provided, thus drastically reducing risk.

Trusted Access Manager for Z from Broadcom streamlines the management of privileged IDs on the mainframe and allows these users to elevate their privileges *just in time* for critical work, and then return to a non-privileged state after work is completed. This functionality can be provided manually, based on time, or even associated with service desk tickets.

Clean Up the Security Database to Reduce Exposure from Over-Provisioned Accounts

Mainframe access, and its security, are based on a foundation of IDs and associated entitlements. Mainframe's longevity and criticality typically result in these records adding up over the years. More critically, users often retain the same ID when moving to different roles or responsibilities resulting in an ID with too many entitlements. This practice results in potential exposures as entitlements go unused and forgotten and also deviates from *least access principles*.

Should a credentials be stolen, it can often be difficult to understand what is at risk or what may have been breached, especially when the compromised ID has outdated entitlements that have accrued over years.

By reducing the number of unused and redundant entitlements, we follow the best practice of least access principles and reduce exposure of mainframe assets in the event that credentials are stolen or misused.

Cleanup from Broadcom monitors entitlement use over time and provides recommendations for rarely or never used entitlements. It provides the ability to remove these obsolete, unused, redundant, and excessive access rights through an automatable process. The process provides built-in fallback of removed entitlements and IDs, thus cleaning up your mainframe security databases.

Better Protection of Your Mainframe from Phishing Attacks

Increasing the resilience of mainframe to phishing attacks is vitally important. We have outlined the following best practices for better resilience:

- Use multi-factor authentication on critical applications, groups or accounts.
- Manage privileged users with a privileged access management solution.
- Clean up mainframe security databases to reduce exposure from over-provisioned accounts.

All these best practices can be easily enabled through implementation of Advanced Authentication Mainframe, Trusted Access Manager for Z, and Cleanup, resulting in better protection for your mainframe from phishing attacks.

For more information about these products, please visit the following product pages:

- Trusted Access Manager for Z: www.broadcom.com/products/mainframe/identity-access/trusted-access-manager-for-z
- Advanced Authentication Mainframe: techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-advanced-authentication-mainframe/2-0.html
- Cleanup: www.broadcom.com/products/mainframe/compliance-data-protection/cleanup

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

MF-PHRES-SB100 June 20, 2022