Pension Services – OCC Cyber Security

Scope

This report aims to cover the high-level security posture of any OCC-maintained Pension Services infrastructure, namely the following:

- "R Drive" – The Pension Services shared drive.
- Bottomline/PTX Server.

The service relies heavily on externally hosted software managed by third-party providers. This limits the checks that ITID can perform in-house. To address this, we have proactively sought information directly from the suppliers to assess their security posture. This includes reviewing penetration test reports and any security certifications. There are no concerns with any of the information provided or the wider security posture from these providers.

Summary

No critical security issues have been identified. All outstanding software vulnerabilities are to be expected, in line with expected patching cycles and will be addressed as part of business-as-usual maintenance.

The Bottomline/PTX Server was migrated to Windows Server 2022 in September 2023, this work has extended the lifecycle of the server and ensured that it will remain supported and secure until at least 2031.

Vulnerabilities

This includes a check for any technical, software vulnerabilities, covering the Operating System and any supported applications.

- The "R Drive" has no significant security vulnerabilities.

- The Bottomline/PTX server has no outstanding vulnerabilities, following regular scheduled maintenance which took place on Sunday January 28th, 2024.

Access Control

- Access to the R drive is marked as 'Restricted', subject to approval from Sean Collins or Sally Fox. 45 colleagues currently have access.

- Access to the 'PTX-DataIn' folder on the Bottomline/PTX server is restricted to the following individuals: Sally Fox, Rachael Salsbury, Amy Middleton and Jeanette Thomas.

Outstanding actions

We currently have an outstanding action to implement Single Sign-On for the Bottomline application. Once completed, this initiative will simplify our access to the service and improve the security. It will eliminate the necessity for a manual 'leavers' process and provide ITID with auditing capabilities. Furthermore, real-time advanced security checks will be applied to identify potential risks, such as 'impossible travel detection' and instances where staff access the application from unusual locations or devices.

This is awaiting technical details from the 3rd party, and implementation planning and governance from ITID. This work is scheduled to take place in Q1 2024.