Security Review of Data Linkage Systems 2017

Introduction

In January 2017, the Data Linkage Branch (DLB) contracted an independent security review of its systems and processes, carried out by Asterisk Information Security. The scope of the review comprised all systems and resources within the remit of DLB.

Asterisk Information Security

Asterisk Information Security (Asterisk) is a specialist consultancy providing clients with actionable security advice, guidance and solutions to improve their overall information security.

Asterisk has an absolute focus on security and risk management. Unlike other integrators and professional services organisations that offer information security as a subset of their many service lines, Asterisk focuses purely on information security. This focus ensures an understanding of all aspects of security from regulatory issues, governance and audit requirements to technical deployment and integration.

The founding consultants of Asterisk have provided information security advice, services and infrastructure to WA businesses for more than 15 years. Their experience ranges from assisting small and medium businesses to larger enterprises covering sectors such as government, mining and resources, critical infrastructure and commercial. Asterisk is a member of CREST Australia (the Council of Registered Ethical Security Testers).

Review Format

Asterisk reviewed the current security posture of the Western Australian Data Linkage System (WADLS), including associated Data Collections processes, and alignment with the following industry practices and guidelines: ISO/IEC 27002:2013; ASD Strategies to Mitigate Cyber Security Incidents; and SANS Critical Security Controls for Effective Cyber Defence.

The review comprised six stages:

1. **Information gathering** – Asterisk reviewed DLB documentation relating to operating systems; policies and procedures; third party product documentation; high level and detailed design; and security tasks and activities already undertaken.

2. **Systems and Services workshop** – Asterisk gained understanding of the DLB, WADLS, and core DOH Data Collections through discussions with staff.

3. **Security Processes and Controls workshop** – Asterisk leveraged the information provided in the previous workshop to determine appropriate security controls throughout the WADLS.

4. **Threat Modelling workshop** – Asterisk developed applicable risk scenarios and assessed each one in terms of risk level and existing controls.

5. **Analysis** – Asterisk undertook a detailed analysis of all workshop findings, including controls, documentation, and statements from personnel to identify potential control gaps.

6. **Report** – Asterisk delivered a presentation of findings, including a prioritised list of recommendations to improve Information Security Management at DLB.

Outcomes

Asterisk assessed 18 threat scenarios and graded their current risk levels, with zero scenarios graded as "High Risk", eight as "Medium Risk" and ten as "Low Risk".

Additionally, Asterisk delivered 17 recommendations for improving Security at DLB. These were rated according to their level of importance, with three recommendations rated as "High Importance", ten as "Medium Importance" and four as "Low Importance".

Next Steps

DLB is now working on implementing the recommendations presented in the Asterisk report. Implementing these recommendations will help mature the Information Security posture within DLB through the optimisation of existing processes.

Links

- Privacy and Security at the Data Linkage Branch: http://www.datalinkage-wa.org.au/privacy-and-security
- Asterisk Information Security: https://www.asteriskinfosec.com.au/

Contact

For more information, please contact the Manager, Data Linkage Systems:

Tom Eitelhuber
E: tom.eitelhuber@health.wa.gov.au
T: (08) 9222-2371

healthywa.wa.gov.au