Use Case : Security Risk Assessment & Audit (SRAA)

mandata@cyberservices.com

New Financial Management System Implementation for NGO

Background

A social service NGO with multiple office & service center locations in Hong Kong deployed a new financial management system in Q1 2019. To observe Hong Kong OCGIO requirements on *Security Risk Assessment & Audit* (SRAA) upon new system implementation, we were engaged as the third-party assessor to perform independent SRAA based on *Practice Guide for Security Risk Assessment & Audit* (ISPG-SM01, version 1.1) released by OCGIO by November 2017.

保安風險評估程序 Security Risk Assessment Process + 保安審計 Security Audit

就電腦系統的保安問題，社署於社會福利發展基金第三階段撥款鼓勵機構為新建構的系統進行保安風險評估及審計(SRAA)，機構可聘請第三方獨立顧問，於完成系統建構後，為系統進行保安風險評估及審計，提供相關報告及改善建議。

Challenges

- There are limited time and resources, we need to set the focus areas & resources
- On the other end, it is intended to mitigate and manage security risks as comprehensive as possible

Our Solutions & Deliverables

- **Focused Scope** - we tuned the SRAA to have specific focus as the **pre-production assessment** for the new Financial Management System Implementation; but not a replcement of regular IT / IT security control review.
- **ZERO delay to the implementation** - we delivered highly dedicated resources and finished the whole assessment within a short period of time, made ZERO delay to the implementation shedule.
- **Comprehensive remediation recommendation walk-thru** – we organized comprehensive remediation recommendation walk-thru session to assist our clients in understanding the findings & the recommended remediation

Risk Rating	Description
Non-Compliant	(i) Significant Risk on confidential data (ii) operation critical systems
Basic Minimum	Overall risk level is acceptable, with no issue (i) or (ii) stated above
Standard	No Remediation Required

Risk Rating Assessment Methodology

RISK Rating		Data Type		Network		Business Operation		IT Security verified Scanned Result
Non-Compliant	=	Confidential	X	External	X	Operation Critical	X	Critical / High
Basic Min		Internal		Internal		Operation Support		High / Medium
Standard		Public				Non-Operation / Non-Production		Medium / Low

#12	
Risk:	Low
Finding:	Query Parameter in SSL Request
Detail:	Query parameters were passed over SSL, and may contain sensitive information. It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted.
Affected area:	116 items (Referred to AppScan report)
Recommendation:	Always use SSL and POST (body) parameters when sending sensitive information.
Supporting:	N/A

#13	
Risk:	Low
Finding:	Robots.txt File Web Site Structure Exposure
Detail:	The web server or application server are configured in an insecure way. It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site.
Affected area:	http://www.v
Recommendation:	Move sensitive content to an isolated location to exclude it from web robot search
Supporting:	N/A