CHECK
IT Health Check Service

DigitalAssurance

Security Assessment Report

Disclosure Scotland - Glasgow

Produced for British Telecommunications

BT

Version: 1.0 DRAFT
Date: 29 March 2018
CHECK Team Leader: [redacted]
CHECK Ref: 10591

OFFICIAL SENSITIVE

Management Report

Introduction

This report details the findings and recommendations from an IT Security Assessment conducted by Digital Assurance (DA) for British Telecommunications (BT) in March 2018. The security assessment was conducted against the Disclosure Scotland - Glasgow systems under the terms of the NCSC CHECK scheme.

It is important to bear in mind that security assessment reports such as this are exception-based reports and as such generally document identified security flaws rather than identifying security controls that may have performed well.

Summary

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Vulnerability Root-cause	Total	Risk Rating				
		Critical	High	Moderate	Low	Info
All Categories	**44**	**-**	**8**	**16**	**19**	**1**
Application Software	6	-	-	-	5	1
Database Configuration	-	-	-	-	-	-
Host Configuration	13	-	2	2	9	-
Firewall Configuration	3	-	-	1	2	-
Infrastructure Design	-	-	-	-	-	-
Password Policy	1	-	-	1	-	-
Patch Management	16	-	5	10	1	-
Other	5	-	1	2	2	-

Key Findings

The most significant security issues identified during this assessment are summarised here, additional detail is provided in the 'Technical Summary' component of this management report and the 'Detailed Findings and Recommendations' section of this document.

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]

Key Recommendations

Suggested remedial actions for the key security issues are summarised here, additional detail is provided in the 'Detailed Findings and Recommendations section of this document.

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]

Summary of findings

The findings of the assessment are summarised below alongside the current status of each finding at the time of report issue.

Infrastructure Testing						
Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Closed
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open

Infrastructure Testing

Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open

Host Configuration Security Review

Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open

Firewall Configuration Security Review

Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	High	Low	Moderate	Open
[redacted]	[redacted]	[redacted]	Moderate	Moderate	Moderate	Open
[redacted]	[redacted]	[redacted]	Low	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open

Infrastructure Testing						
Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	Low	Low	Low	Open

Web Application Testing						
Ref	Issue	Action	I	L	Risk	Status
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	High	Moderate	High	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Low	Low	Low	Open
[redacted]	[redacted]	[redacted]	Low	Low	Low	Open
[redacted]	[redacted]	[redacted]	Low	Low	Low	Open
[redacted]	[redacted]	[redacted]	Moderate	Low	Low	Open
[redacted]	[redacted]	[redacted]	Information	Information	Information	Open

Document Control

Reference	DAEC3537
Version	1.0 DRAFT
Creation Date	29 March 2018
Last Update	13 April 2018
Protective Marking	**OFFICIAL SENSITIVE**
Author	[redacted]
Authorisation	[redacted]

[redacted]

[redacted]

Name	Organisation	Copy Number
Electronic Copy	Digital Assurance	01
[redacted]	British Telecommunications	02
CHECK	NCSC	03

Table 2 : Document distribution

Version History

Date	Author	Version	Reason for Update
29/03/2018	[redacted]	DRAFT v0.1	Document created
09/04/2018	[redacted]	DRAFT v0.2	Review and QA
11/04/2018	[redacted]	DRAFT v0.3	QA Amendments
13/03/2018	[redacted]	DRAFT v1.0	Release

Table 3 : Document version history

Confidentiality and Copyright

The information contained in this report is confidential and is submitted by Digital Assurance Consulting Ltd (Digital Assurance) on the understanding that it will be used only by the Staff and, where relevant, suppliers of British Telecommunications. In particular, the contents of this document may not be disclosed in whole or in part to any other party without the prior written consent of Digital Assurance.

Validity of Information

Digital Assurance has made every effort to ensure that all statements and information contained herein are accurate however it should be noted that the results of security testing reflect the systems as they were at the time of the testing and as such represent a 'snapshot' of the systems during the assessment.

[redacted]

Using This Report

This report is intended to provide details of the findings and recommendations arising from information security assessment activities (e.g. penetration testing, systems review or application security testing) conducted by Digital Assurance.

The report is designed to communicate important and sensitive information regarding security issues to both technical and non-technical staff with a requirement to know details or particular aspects of the security assessment findings.

Report Structure

The report is split into a number of sections to maintain structure and enhance readability as follows:

Introduction	This section contains background information regarding the parties, nature of the engagement as well as a brief overview of Digital Assurance security assessment services.
Scope	This section of the report details the objectives of the assessment with regard to type of testing performed and target systems/networks for the assessment. The scope section also documents any constraints and limitations in place during the testing.
Approach	This section outlines the overall approach taken to undertaking the security assessment
Detailed Findings and Recommendations	This section of the report provides detail on each individual issue identified during the assessment along with affected components, risk description, impact, likelihood and risk ratings along with a recommendation and estimated effort to implement recommendations. Often, detailed issues will reference appendices or external files especially where supplementary data is provided or where issues are broken down further into sub-issues.
Summary and Conclusion	This section summarises and consolidates the recommendations arising from the technical testing. Where appropriate, recommendations are provided that address the root cause of identified issues rather than to simply tackle each issue as a discrete fix. The aim is to provide recommendations that prevent re-occurrence of the issues.
Appendices	Appendices generally contain further technical details and often provide a level of detailed information on systems or

	vulnerabilities identified that would be inappropriate for the main detailed findings section.

Presentation of Issues and Findings

Issues are presented in a common format to aid readability and assist the client in prioritising issues and, importantly, prioritising remedial action where necessary. The common issue presentation format contains a number of fields describing the nature of the issue, risk and recommendation as follows:

Reference	Unique identifier for the issue. Every issue in every Digital Assurance report you receive will be assigned this unique identifier which aids issue tracking.
Title	Short form title summarising the security issue
Testing phase	Documents from which phase of the testing the issue originated. This may be External testing, Internal testing, DMZ testing etc.
Impact rating	A rating of the likely impact resulting from a successful attack or exploitation of the issue. Ratings run Low, Moderate, High and Critical. An additional category of Info
Likelihood rating	A rating of the likelihood of a successful attack, this incorporates parameters such as availability of exploit code, complexity of attack and compensating controls/mitigating factors. Ratings run Low, Moderate and High.
Risk rating	An overall rating of the 'technical risk' posed by the issue. This is generally decided by both the impact and the likelihood although it is subject to modification based on other factors considered by the security assessor. Ratings run Low, Moderate, High and Critical. The rating of Information is used for informational issues.
Fix effort	A rating of the anticipated effort required to successfully perform remediation work, generally based on the recommendations made for a specific issue. This rating is highly subjective but is based on the security assessor's experience of similar issues and organisations. Ratings run Low, Moderate and High. This can loosely be translated to man-days as follows: 1. *Low*: up to 1 man-day of effort 2. *Moderate*: up to 5 man-days of effort 3. *High*: over 5 man-days of effort
Issue	A description of the security issue.

Affected Components	Where applicable this will detail the systems, applications or other components affected by the issue. Where an issue is prevalent throughout a large population of components this may simply state that the issue is widespread.
Risk	A description of the risk posed generally detailing the attacker type, attacker pre-requisites and the likely impact on information assets.
Recommendation	A recommendation or set of recommendations for remediation or otherwise mitigating the risks posed by the issue.
Notes	Any additional observations or other notes relating to the issue.
References	Any vendor, CVE and other references relating to the issue.

Introduction

Digital Assurance was engaged by British Telecommunications to undertake a security assessment of the Disclosure Scotland - Glasgow systems and associated infrastructure. The assessment was performed in March 2018 and consisted of 4 phases of technical assessments as summarised below:

- Infrastructure Testing
- Host Configuration Security Review
- Firewall Configuration Security Review
- Web Application Testing

All security testing was performed at BT Disclosure Scotland Newcastle (CTE) and Glasgow (PQ) by [redacted] of Digital Assurance between Monday 05 March and Wednesday 28 March 2018.

About Digital Assurance

Digital Assurance is a London based security consultancy delivering a range of security assessment, secure design and security training services. Digital Assurance was founded in 2006 by experienced and well-respected security consultants who have been delivering information security and assurance services to UK and international clients for over a decade.

Our security assessments are generally highly tailored to customer requirements and are designed to provide the greatest level of assurance for a given amount of time and budget.

Digital Assurance is a UKAS accredited ISO9001:2008 organisation. Digital Assurance is an NCSC CHECK scheme subscriber and authorised to conduct testing on government systems under the terms of the CHECK scheme.

ISO 9001
BUREAU VERITAS
Certification
UKAS
008

CHECK
IT Health Check Service

Scope

The scope of work is documented in this section of the report for each stage of the assessment and where relevant will reference external scope documents.

The scope of work was agreed between Digital Assurance and British Telecommunications and is detailed in the Terms of Reference (ToR) document associated with this security assessment.

BT Disclosure Scotland - Glasgow

Infrastructure Testing

PQ Ops VLANS		
VLAN ID	Network Range	Network Label
[redacted]	[redacted]	Log Collect Production
[redacted]	[redacted]	Log Collect Management
[redacted]	[redacted]	HP Openview
[redacted]	[redacted]	VPN1
[redacted]	[redacted]	VPN2
[redacted]	[redacted]	VPN3
[redacted]	[redacted]	VPN4
[redacted]	[redacted]	Mail
[redacted]	[redacted]	IL4 Management
[redacted]	[redacted]	Infrastructure Services
[redacted]	[redacted]	Infrastructure Services Management
[redacted]	[redacted]	Infrastructure Services SAN
[redacted]	[redacted]	Nokia Firewall Management
[redacted]	[redacted]	Infrastructure Services Private
[redacted]	[redacted]	Terminal Services
[redacted]	[redacted]	Hyper-V SAN
[redacted]	[redacted]	Hyper-V Infrastructure Services
[redacted]	[redacted]	Internet Data
[redacted]	[redacted]	Network Management

PQ Support VLANS		
VLAN ID	Network Range	Network Label
[redacted]	[redacted]	Database
[redacted]	[redacted]	RAC Cluster 1 Private
[redacted]	[redacted]	RAC Cluster 2 Private
[redacted]	[redacted]	Internet Presentation Back
[redacted]	[redacted]	Internet Presentation Management
[redacted]	[redacted]	Database Management
[redacted]	[redacted]	Application
[redacted]	[redacted]	Application Private
[redacted]	[redacted]	Application Management

[redacted]	[redacted]	MIS
[redacted]	[redacted]	MIS Private
[redacted]	[redacted]	MIS Management
[redacted]	[redacted]	Intranet Proxy
[redacted]	[redacted]	Intranet Presentation Front
[redacted]	[redacted]	Intranet Presentation Back
[redacted]	[redacted]	Internet Proxy
[redacted]	[redacted]	Internet Presentation Front
[redacted]	[redacted]	Intranet Presentation Management
[redacted]	[redacted]	MPX SAN
[redacted]	[redacted]	IL3 iLO
[redacted]	[redacted]	IL4 iLO
PQ Live VLANS		
VLAN ID	Network Range	Network Label
[redacted]	[redacted]	IL3 ILO
[redacted]	[redacted]	IL4 ILO
[redacted]	[redacted]	MIS
[redacted]	[redacted]	MIS Private
[redacted]	[redacted]	MIS Management
[redacted]	[redacted]	MIS SAN
[redacted]	[redacted]	HPOV RAC Cluster Private
[redacted]	[redacted]	Database Management
[redacted]	[redacted]	Database
[redacted]	[redacted]	Application Management
[redacted]	[redacted]	Application SAN
[redacted]	[redacted]	Application
[redacted]	[redacted]	Mail Gateway Management
[redacted]	[redacted]	Mail Gateway
[redacted]	[redacted]	Terminal Services - Live
[redacted]	[redacted]	RAC Cluster 1 Private - De-scoped
[redacted]	[redacted]	RAC Cluster 2 Private - De-scoped
[redacted]	[redacted]	Application Private
[redacted]	[redacted]	Internet Presentation Back
[redacted]	[redacted]	Print and Scan DMZ
[redacted]	[redacted]	Intranet Proxy
[redacted]	[redacted]	Intranet Presentation Front
[redacted]	[redacted]	Intranet Presentation Back
[redacted]	[redacted]	Hyper-V Infrastructure Services
[redacted]	[redacted]	Pacific Quay Standalone Management
[redacted]	[redacted]	Pacific Quay Standalone IL4
[redacted]	[redacted]	Pacific Quay Standalone terminals
[redacted]	[redacted]	Internet Proxy
[redacted]	[redacted]	Internet Presentation Front
[redacted]	[redacted]	Internet Mail Gateway Management
[redacted]	[redacted]	Internet Mail Gateway