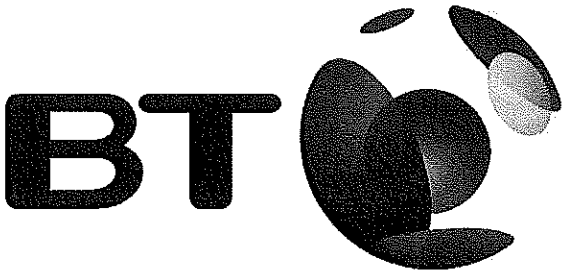
DigitalAssurance

Security Assessment Report

PCI Newcastle CTE Network Vulnerability assessment

Produced for BT Group PLC



Version: 1 0 DRAFT
Date: 08 August 2016

Management Report

Introduction

This report details the findings and recommendations from an IT Security Assessment conducted by Digital Assurance (DA) for BT Group PLC (BT) in August 2016. The security assessment was conducted in Newcastle against the PCI systems located in Glasgow, Scotland.

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

In general, both the infrastructure and the systems located within it were found to be well configured with regard to security with the majority of key security controls functioning as expected. [redacted]

[redacted]

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

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]

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]

Summary of findings

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

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

Document Control

Reference	DAPR3404
Version	1.0 DRAFT
Creation Date	08 August 2016
Last Update	15 August 2016
Protective Marking	OFFICIAL - SENSITIVE
Author(s)	[redacted]
Authorisation	[redacted]

Table 1 : Document control

Distribution

Name	Organisation	Copy Number
Electronic Copy	Digital Assurance	01
[redacted]	British Telecoms	02

Table 2 : Document distribution

Version History

Date	Author	Version	Reason for Update
08/08/2016	[redacted]	0.1 DRAFT	Document created
12/08/16	[redacted]	0.2 DRAFT	QA
12/08/16	[redacted]	0.3 DRAFT	Amendments following QA
15/08/16	[redacted]	1.0 DRAFT	Release

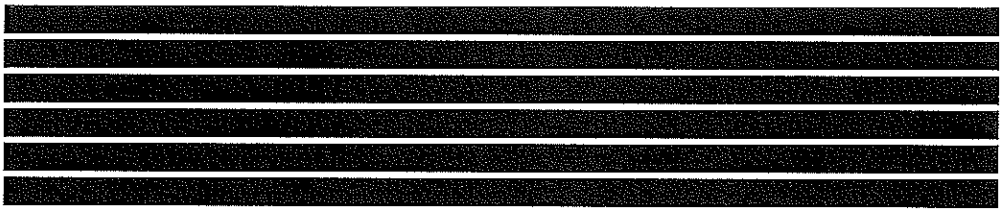
Table 3 : Document version history

Confidentiality and Copyright

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.

Contents



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 BT Group PLC to undertake a security assessment of the PCI systems and associated infrastructure. The assessment was performed in August 2016 and consisted of 1 phase of technical assessment as summarised below:

- [redacted]

All security testing was performed at the Carliol Square CDE premises by [redacted] an [redacted] of Digital Assurance on Thursday 4 August 2016.

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 and is the only UK based organisation that has successfully undertaken and received the CESG Claims Tested Mark (CCTM) award for security testing services, the CCTM represents a UK government quality assurance mark for security products and services.

Digital Assurance is a CESG CHECK scheme subscriber and authorised to conduct testing on government systems under the terms of the CHECK scheme. Digital Assurance also provide CLAS consultancy throughout the public sector.

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 Telecoms and is detailed in the Terms of Reference (ToR) document associated with this security assessment.

Infrastructure Testing

A sample of 4 VLAN segments containing hosts intended to be PCI-compliant was selected for a vulnerability assessment:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Approach

Infrastructure Testing

Phase One - Network Enumeration

Digital Assurance will attempt to map the network and identify relevant active nodes or potentially sensitive service clusters within it. Systems and networks will be classified in terms of their importance as hosting potentially sensitive information assets.

Phase Three – Vulnerability Analysis

Next, the ports and services that have been revealed on the systems will be reviewed for vulnerabilities. Using our consultants' knowledge and experience as well as common and private sources of vulnerability and exploit information, Digital Assurance will produce a map of the services that are present on the systems with any potential vulnerabilities that could lead to an exploitation of them.

The results of the vulnerability analysis will be discussed with the client, particularly with regard to minimising the onward risk of affecting service. Areas such as account lock outs and the possibility of system / application crash due to exploit techniques (e.g. buffer overflow attacks) will be explained and ruled in or out of the proceeding phases.

Detailed Findings and Recommendations

Infrastructure Testing findings

[redacted]

Impact	Moderate	Likelihood	Moderate	Risk	Moderate
Category	Patch Management			Fix Effort	Low

Issue Description

[redacted]

Components Affected

The following hosts were noted to contain the above issues:

[redacted]

Risk Description

[redacted]

Recommended Action

[redacted]