MAZARS CROYDON

Final Internal Audit Report

Unix (Linux) Operating System Security

February 2018

Distribution:

Executive Director Resources (Final only)
Head of ICT
ICT Service & Contract Manager

Assurance Level	Issues identified	
Substantial Assurance	Priority 1	0
	Priority 2	1
	Priority 3	2

Status of Our Reports

This report ('Report') was prepared by Mazars Public Sector Internal Audit Limited at the request of the London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, we have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of the London Borough of Croydon and to the fullest extent permitted by law, Mazars Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility set out in appendix 3 of this report for further information about responsibilities, limitations and confidentiality.

Contents

Page

Executive Summary

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 The Council's network infrastructure, including server operating system security, is managed by its IT service provider, Capita. As part of this year's plan, an internal audit in respect of the Unix (Linux) Operating System (m01croydongovuk) in use by the Council was selected as a sample of the security configuration applied to the operating system.

1.2 This audit is part of the Internal Audit Plan for 2017/18. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Issue
Management should ensure that powerful usernames are prevented from using FTP (File Transfer Protocol), **(Rec 1).**

Priority 3 issues are detailed under item 4.

3. Actions and Key Findings/Rationale

<table>
<tr><td colspan="4"><b>Control Area: Use of FPT</b></td></tr>
<tr><td><b>Priority</b></td><td colspan="2"><b>Action Proposed by Management</b></td><td><b>Detailed Finding/Rational – Issue 1</b></td></tr>
<tr><td>2</td><td colspan="2">A project to deprecate the Mobile Iron infrastructure has been approved and is in delivery, our supplier will decommission the legacy infrastructure once all managed devices are transitioned to our target cloud-based MDM solution</td><td rowspan="3">The File Transfer Protocol (FTP) allows the transfer of files between systems. However, it also has a number of security concerns associated with it, including allowing users unlimited attempts to log in to an account. Preventing users from accessing the system via FTP provides assurance that system resources and information are not unnecessarily exposed to unauthorised access, tampering and damage.
SekChek analysis run on the UNIX operating system identified 37 users on the system. Although only one user is active, we established that no usernames are prohibited from accessing the system via FTP which mean powerful usernames such as 'ROOT' can be used to access the system via FTP.
File transfer via FTP is transferred in clear text and is not encrypted, which could mean that passwords are intercepted. If powerful usernames are allowed to access the system via FTP, there is an increased risk that system resources and information are unnecessarily exposed to unauthorised access, tampering and damage.</td></tr>
<tr><td colspan="2"><b>Responsible officer</b></td><td><b>Deadline</b></td></tr>
<tr><td colspan="2">ICT Business Continuity &amp; Security Officer</td><td>April 2018</td></tr>
</table>

4. Priority 3 Issues

Agreed Action/s	Detailed Finding / Rationale
A project to deprecate the Mobile Iron infrastructure has been approved and is in delivery, our supplier will decommission the legacy infrastructure once all managed devices are transitioned to our target cloud-based MDM solution in April 2018.	From the *SekChek* analysis, it was noted that a number of security policies and parameters had not been appropriately configured in line with leading practice and consistently applied to usernames defined on the system, including the: • Minimum Password length is set at 5 characters; • Maximum Password Change Interval has not been set; and • SU attempts are not logged, therefore switching of users access to 'root' access will not be identified. Unless effective security settings are established and applied in the LINUX Server operating system, there is an increased risk that system security could be compromised.
A project to deprecate the Mobile Iron infrastructure has been approved and is in delivery, our supplier will decommission the legacy infrastructure once all managed devices are transitioned to our target cloud-based MDM solution in April 2018.	From the *SekChek* analysis, it was noted that 35.7% (20) of the 56 groups defined on the system were redundant and did not contain any members. Although this is a housekeeping issue, there is risk that unnecessary groups exist on the server, which could be abused and used to exploit security on the system.

Appendix 1

TERMS OF REFERENCE

Unix (Linux) Operating System Security

1. INTRODUCTION AND BACKGROUND

1.1 The Council's network infrastructure, including server operating system security, is managed by its IT service provider, Capita. As part of this year's plan, an internal audit in respect of the Unix (Linux) Operating System for a key system in use by the Council will be selected as a sample of the security configuration applied to the operating system.

1.2 The scope of this audit will look at the security configuration of a sample Unix (Linux) Operating System with the aid of the SekChek security analysis tool.

1.3 This audit is part of the agreed Internal Audit Plan for 2017/18.

2. OBJECTIVES AND METHODOLOGY

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness control framework operating

2.2 In order to achieve the overall objective, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate testing. Comparison will be made as appropriate with best practice guidance.

3. SCOPE

3.1 This audit examined the following areas, (and number of issues identified):

Audit Area	Issues Identified		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
System Wide Security Policy;	0	0	1
Trusted Users;	0	0	0
Use of FTP;	0	1	0
Analysis of Usernames;	0	0	1
Analysis of Groups;	0	0	0
Login Script File;	0	0	0
World Writeable Files;	0	0	0
SUID Permissions;	0	0	0
SGID Permissions;	0	0	0

Network Services; and	0	0	0
Trusted Hosts.	0	0	0

Appendix 2

DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

🟢	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
🟡	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
🟠	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
🔴	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

Appendix 3

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.