MAZARS

CROYDON

Final Internal Audit Report

SekChek Active Directory System Security

August 2018

Distribution:

Executive Director Resources (Final only)
Chief Digital Officer
ICT Service & Contract Manager
Senior Transformation and Service Improvement Manager
Enterprise Architect
Talent Pool
Cloud Security Solutions Architect

Assurance Level	Recommendations Made	
Limited Assurance	Priority 1	0
	Priority 2	9
	Priority 3	1

Status of Our Reports

This report ("Report") was prepared by Mazars Public Sector Internal Audit Ltd at the request of 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 internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit 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 London Borough of Croydon and to the fullest extent permitted by law Mazars Public Sector Internal Audit Ltd. 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 in Appendix 3 of this report for further information about responsibilities, limitations and confidentiality

Contents

Page

Executive Summary

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 Active Directory was selected as a sample of the security configuration applied to the IT systems of the Council (i.e. those systems that require Active Directory log in to gain access).

1.2 The scope of this audit looked at the configuration of the security policies defined in Active Directory with the aid of the SekChek security analysis tool.

1.3 This audit was 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 Issues
431 network accounts had administrative privileges, **(Issue 1.)**
Network passwords are required to be changed every 90 days, 19% of users are not required to change their passwords and for 3% of accounts the password can only be changed by a security administrator, **(Issue 2.)**
62% of accounts have not logged into the network for the last 3 months and some of these accounts have not logged in since 2003, **(Issue 3.)**
1% of users are allowed to logon with a zero length password due to the security settings configured in individual user accounts, **(Issue 4.)**
The lockout threshold was set to 12; and 1.6% of user accounts were locked out, **(Issue 5.)**
Auditing was not enabled for 17 out of 29 auditable events, as recommended by Microsoft for a strong and secure environment, **(Issue 6.)**
57.4% of the installed services had stopped **(Issue 7.)**
17.5% of the Local Security groups were empty (i.e. they have no members); and 0.1% of the members were defined in other domains, **(Issue 8.)**
25.5% of the Global Security groups were empty (i.e. they have no members), **(Issue 9.)**

The Priority 3 issue is detailed under item 3 below.

3. Actions and Key Findings/Rationale

<table>
<tr><td colspan="4"><b><u>Network accounts with Administrative Privileges</u></b></td></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 1</th></tr>
<tr><td>2</td><td colspan="2">A review of accounts with administrator privileges was performed in January 2018, this will inform any action needed to reduce the number of accounts with Admin privileges as appropriate
Reviews will continue be performed at least annually.
A large number of accounts with administrator privileges are still necessary. A subset of the 431 accounts identified were also likely to be disabled AD accounts.</td><td rowspan="3">The Administrator privilege is the most powerful privilege in the domain and has full control over the domain resources. The number of accounts with Administrator privilege should be kept to a minimum and only be used for administrative functions. Users with administrative privileges should use a separate account for their normal day-to-day use.
The inspection of the user accounts defined in the domain noted that 4% (431) of 11,722 user accounts have 'Administrative' privileges.
If users belong to groups with permissions and rights greater than they need, they will have access to resources and system functions not in line with their job functions.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="3"><u>Passwords - maximum age, never expire and users are not allowed to change</u></th></tr>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 2</th></tr>
<tr><td>2</td><td>LBC uses a combination of security controls to mitigate the findings mentioned. This includes, but is not limited to, a mixture of the following:
- Enforced password complexity and history for all stated accounts
- Fine-grained password policy with increased complexity (14 character) for Admin and Service Accounts
- multi-factor authentication for Admin and user accounts using a combination of trusted device and user account, or One-Time passcode
- Complementary Administrative control with ICT security policy mandating password secrecy and good practice
The above prevent compromise in the unlikely event of password disclosure.</td><td rowspan="3">In order to ensure security and integrity of the network, end users should be prompted to regularly change their passwords. Current leading practice across a range of industry sectors, recommends users to change their passwords every 30 to 60 days. For service accounts that do not need to have their passwords changed on a frequent basis, the account name and password should be of sufficient length and complexity, making them difficult to guess.
Inspection of the Domain Account Policy and user accounts noted that:
• Network passwords are required to be changed every 90 days;
• 19% (2,239) of 11,722 users are not required to change their passwords. It is acknowledged that for some service accounts, it is necessary for their passwords to remain the same, to prevent a disruption in the service being provided; and
• For 3% (410) of 11,722 accounts the password can only be changed by a security administrator.
If users are not required to change their passwords on a frequent basis, their passwords may become known to other employees and/or potential intruders. The user profile could then be used to gain unauthorised access to the network, impacting on system security and data integrity.</td></tr>
<tr><th>Responsible officer</th><th>Deadline</th></tr>
<tr><td>Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="4"><u>Accounts which have not logged in for more than 90 days</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 3</th></tr>
<tr><td>2</td><td colspan="2">A regular process has been initiated to permanently delete any disabled account that has not been used for over 90- days.
No further action to be taken.</td><td rowspan="3">In order to help prevent unauthorised system access, the user accounts for staff leavers are required to be disabled.
Inspection of user account logons, noted that 62% (7,246) of 11,722 accounts have not logged into the network for the last 3 months and some of these accounts have not logged in since 2003.
Inactive user accounts are a prime target for external and internal intruders. If the passwords to these accounts have been compromised, the accounts could be used without detection, thus impacting on the security and integrity of the network.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="4"><u>Accounts not requiring a password</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 4</th></tr>
<tr><td>2</td><td colspan="2">Accounts with zero length passwords will be reviewed and will be dealt with as appropriate.</td><td rowspan="3">It is Council Policy that all user accounts have an appropriate password in place, although some system accounts will have zero-length (null) passwords. The setting that allows zero-length (null) passwords to be defined at user account level is one of the values that cannot be displayed via the standard Windows 'Active Directory Users' interface. It can only be displayed (or set) via a special interface.
An Administrator can set passwords for the listed accounts to null regardless of domain-level security settings. The accounts could then be used to login to the system without a password, despite the security policy settings defined at domain-level. However, the system will not allow users to change their own passwords to null provided that domain-level security settings prevent it. This can only be done by an Administrator via the 'Reset Password' function or via a special interface.
Inspection of user accounts noted that 1% (124) of 11,722 users are allowed to logon with a zero length password due to the security settings configured in individual user accounts.
There is a risk that some user accounts inappropriately have zero length passwords and that inappropriate system access may be gained through these.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>30 September 2018</td></tr>
</table>

<table>
<tr><th colspan="3"><u>Lockout threshold and user accounts locked out</u></th></tr>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 5</th></tr>
<tr><td>2</td><td>The lockout threshold will be reviewed.</td><td rowspan="3">Croydon's ICT policy, paragraph 20.3.1, states that, 'To prevent password guessing attacks, the number of login attempts must be restricted and failed attempts logged. After five unsuccessful attempts to enter a password the user account must be locked. Users will either need to contact the Service Desk to have access re-established or the account lockout expires after 30 minutes and access is re-enabled. If a breach of log on controls is detected, a security incident must be logged and investigated'

Through inspection of the 'Lockout Threshold', i.e. the number of failed attempts at logging in to the network, and the number of locked out accounts at the time the scan was run, it was identified that:

• The lockout threshold is currently set to 12; and
• 1.6% (182) of 11,722 user accounts were locked out.

The higher the value of the lockout threshold, the greater the risk that an end user or intruder, will have more attempts at trying to logon to the network, before they are locked out. However, it should also be noted that if this parameter is set to 0, then the end user or intruder will get an unlimited number of attempts at attempting to logon to the network.

The 182 locked out accounts could be an indication that unauthorised users are trying to gain access to network resources. These unauthorised users could be a mixture of internal users or external intruders.</td></tr>
<tr><th>Responsible officer</th><th>Deadline</th></tr>
<tr><td>Cloud Security Solutions Architect</td><td>30 September 2018</td></tr>
</table>

<table>
<tr><th colspan="3"><u>Audit Policy Settings</u></th></tr>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 6</th></tr>
<tr><td>2</td><td>Although auditing of all events may provide some assistance for some investigations, the total number of events exceeds the storage capability of the event logging system.
This has been reviewed and no further action required.</td><td rowspan="3">Microsoft recommends that the following Audit Policy Settings are enabled for a strong and secure environment:
• Account Logon <i>(Credential Validation, Kerberos Authentication Service, Kerberos Service Ticket Operations, and Other Account Logon Events)</i>;
• Detailed Tracking <i>(DPAPI Activity and Process Creation)</i>;
• DS Access (<i>Directory Service Access on the Domain Controller)</i>;
• Logon and Logoff <i>(Account Lockout, Logoff/Logon, Other Logon/Logoff Events and Special Logon)</i>;
• Policy Change <i>(Authentication Policy Change and MPSSVC Rule-Level Policy Change)</i>; and
• System <i>(IPSec Driver, Security State Change, Security System Extension and System Integrity)</i>.
Through inspection of the Audit Policy Settings, it was identified that auditing was not enabled for 58.6% (17) out of 29 auditable events, as recommended by Microsoft for a strong and secure environment.
Not configuring Audit Policy Settings that monitor the creation or modification of objects, makes it difficult to track potential security threats; and therefore the inability to assign user accountability in the event of a security breach.</td></tr>
<tr><th>Responsible officer</th><th>Deadline</th></tr>
<tr><td>Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="4"><u>Services and Drivers</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 7</th></tr>
<tr><td>2</td><td colspan="2">A review of services running on the Domain controllers was performed in January 2018. Services that were not required had been set to disabled.
Therefore, no further action required.</td><td rowspan="3">A service is an executable object that is installed in a registry database maintained by the Service Control Manager. The executable file associated with a service can be started when the domain controller is booted by a boot program or the Service Control Manager can start it on demand.
Through inspection of the services and drivers installed on the domain controller, it was identified that 441 services were installed. However, at the time of the scan it was noted that 57.4% (253) of these services had stopped.
Having inappropriate or unnecessary services installed, can create security risks and provide potential access paths to tools or intruders.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="4"><u>Domain Local Groups and their Members</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 8</th></tr>
<tr><td>2</td><td colspan="2">Local group membership is used to control access of administrators to local server resources. Membership of these groups was reviewed in January 2018 and will be reviewed annually.
Therefore, no further action required.</td><td rowspan="3">Global groups can be members of local groups in the domain and other domains or members of other global groups in the domain, thus acquiring their rights and granting those rights to users belonging to the global groups.
Through inspection of the Domain Local Groups and their members it was identified that:
• There are 345 Local Security groups, containing 35,184 members;
• 17.7% (61) of these groups are empty (i.e. they have no members); and
• &lt;0.1% (16) of the members are defined in other domains.
If users or groups belong to Local Groups with permissions and rights greater than they need, they will have access to unnecessary resources and functions via the permissions and rights associated with the Local Groups.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>N/A</td></tr>
</table>

<table>
<tr><th colspan="4"><u>Domain Global Groups and their Members</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 9</th></tr>
<tr><td>2</td><td colspan="2">Group membership to be reviewed.
Empty groups to be deleted as appropriate, being empty nominal risk is posed.</td><td rowspan="3">Global groups can be members of local groups in the domain and other domains or members of other global groups in the domain, thus acquiring their rights and granting those rights to users belonging to the global groups.
Through inspection of the Domain Global Groups and their members it was identified that:
• There are 4,971 Global Security groups, containing 293,893 members; and
• 25.5% (1,267) of these groups are empty (i.e. they have no members).
If users are assigned to global groups with permissions and rights greater than they need, they will have access to unnecessary system resources and functions via the permissions and rights associated with the global groups.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Cloud Security Solutions Architect</td><td>30 September 2018</td></tr>
</table>

4. Priority 3 Issues

Action Proposed by Management	Findings
1) The action to delete disabled accounts was stated in the action for the findings above	Through inspection of user accounts, it was identified that 15.6% (1,834) of 11,722 accounts were disabled. Whilst, disabled accounts do not pose a security risk, they should be reviewed and deleted if no longer required (i.e. for housekeeping purposes).

Appendix 1

TERMS OF REFERENCE

Active Directory 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 Active Directory will be selected as a sample of the security configuration applied to the IT systems of the Council (i.e. those systems that require Active Directory log in to gain access).

1.2 The scope of this audit will look at the configuration of the security policies defined in Active Directory 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 and independent opinion on the adequacy and effectiveness of the control framework operating for Active Directory.

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 will examine the following areas:

- System-wide Security Policies;
- Audit Policy Settings;
- Event Logs Settings;
- Registry Key Security Options Settings;
- User Accounts and Passwords;
- Rights and Privileges;
- Trusts and Remote Access;
- Services and Drivers;
- Logical Drives and Network Shares;
- Updates and Patches;
- Discretionary Access Controls; and
- Default Accounts.

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.