

Summary Report: TESTBED AS400

System: S65E570C
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Rating Against Industry Average

		
		X

Overall Comments

Overall, security is below average compared with other AS/400 systems used in the Communications sector.

Report Highlights

Report Section / Comments
<p>2 System Values</p> <p>Most System Values are weak, for example:</p> <ul style="list-style-type: none">OS/400's auditing features are disabled (QAUDCTL, QAUDLVL)Password changes are not enforced (QPWDEXPITV)The minimum password length is only 6 characters (QPWDMINLEN)Users are not prevented from selecting trivial passwords such as 'AAAAA' (QPWDLMTREP)Users are not prevented from reusing old/previous passwords (QPWDRQDDIF)Each character in a new password is not required to be different from the character in the same position in the previous password (QPWDPOSDIF)User passwords are not required to contain numeric characters (QPWDRQDDGT)Users do not receive details of sign-on activity via their profiles (QDPSGNINF)Adjacent numbers are allowed in passwords (QPWDLMTAJC)Users are allowed to sign-on to multiple devices at the same time (QLMTDEVSSN)OS/400's inactivity time-out limits are disabled (QINACTIV)Controls that reduce the risk of intruders gaining access to the system via repeated password guessing attempts are weak (QMAXSIGN)
<p>3 User Profiles and Classes</p> <p>There are 56 user profiles defined on the system.</p> <p>In general, profiles are clearly assigned to specific people.</p>
<p>4 Profiles with Special Authorities</p> <p>The number of profiles with access to the following powerful Special Authorities seems high:</p> <ul style="list-style-type: none">13% (7) of profiles can amend auditing values (*AUDIT)21% (12) of profiles can change system configuration lists (*IOSYSCFG)30% (17) of profiles can control Jobs etc (*JOBCTL) <p>Many of these Special Authorities are acquired via group memberships.</p>
<p>5 Password Change Intervals</p> <p>Password changes are not required for 93% (52) of profiles.</p>
<p>6 Group Profiles and their Members</p> <p>There is only 1 group profile defined on the system.</p>

This report summary is provided to highlight some of the main issues detailed in the SekChek reports. The overall rating is against the industry average and not against leading practice. All comments are generic. For best results they should be considered together with an understanding of the client's own unique business and computer environments.

Summary Report: TESTBED AS400

System: S65E570C
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Report Section / Comments	
8 Passwords Equal to Profile Name	4% (2) of profiles have default passwords. This includes 1 account with security administration (*SECADM) special authority. See the report for implications.
9 Profiles with Expired Passwords	2 profiles have expired passwords and most of these have never been used. See the report for implications.
10 Password Changes	Passwords for 18% (10) of profiles have not been changed in the last 3 months.
11 Last Logons	89% (50) of profiles have not been used in the last 3 months. Some have not been used for several years.
13 Profiles Allowed Simultaneous Device Sessions	100% (56) of profiles can be used to sign-on to multiple devices at the same time.
14 Profiles with Limited Capability	98% (55) of profiles, including several 'regular users' (User Class = *USER) have 'Unlimited Capability'. These users are allowed to change their Initial Program/Menu and to enter OS/400 commands.
16 Profiles without Signon Display Information	100% (56) of users do not receive details of sign-on activity via their profiles.
17 Group and IBM-Supplied Profiles	Some IBM-supplied and Group profiles do not have their passwords set to *NONE.
19 Disabled Profiles	70% (39) of profiles have been disabled or their passwords have been set to '*NONE'.
21 Profiles Created Recently	5 profiles were created in the last 90 days. You should confirm that the creation of these profiles was appropriately authorised by management.
22 Programs with Adopted Authorities	You should check this list for signs of programs that unnecessarily adopt the authority of powerful profiles.
23 Object and Data Authorities	You should check the authorities for the listed Objects, especially those for *PUBLIC access.
24 Network Services	You should check the list of network services to ensure they are valid and required.

This report summary is provided to highlight some of the main issues detailed in the SekChek reports. The overall rating is against the industry average and not against leading practice. All comments are generic. For best results they should be considered together with an understanding of the client's own unique business and computer environments.