the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Microsoft SQL Server 2005

Version 1.1.0
December 2008

Leader:
Mike Taber
Moon River Consulting, Inc.

http://cisecurity.org
feedback@cisecurity.org

Table of Contents

Terms of Use Agreement

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to

distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Introduction

This document is derived from research conducted utilizing the SQL Server 2005 environment on Windows XP Desktops and Windows 2003 servers. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an MS SQL Server 2005 system. With the use of the settings and procedures in this document, an SQL Server 2005 database may be secured from conventional "out of the box" threats. Recognizing the nature of security cannot and should not be limited to only the application; the scope of this document is not limited to only SQL Server 2005 specific settings or configurations, but also addresses backups, archive logs, "best practices" processes and procedures that are applicable to general software and hardware security.

It is extremely important to conduct testing of security configurations on non-production systems prior to implementing them on production systems.

Consensus Guidance

This guide was created using a consensus process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, auditing and compliance, security research, operations, government, and legal.

Configuration Levels

Level-I Benchmark settings/actions

System administrators with any level of security knowledge and experience can understand and perform the specified actions.

The action is unlikely to cause an interruption of service to the operating system or the applications that run on it.

The actions can be automatically monitored, and the configuration verified, by Scoring Tools that are available from the Center or by CIS-certified Scoring Tools**.**

Level-II Benchmark settings/actions

Level-II security configurations vary depending on network architecture and server function. These are of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the operating systems and applications running in their particular environments**.**

Scoring Levels

This section defines the various scoring levels used within this document.

Scorable

This setting or recommendation is able to be assessed by scoring tools or command-line arguments.

Not Scorable

This setting or recommendation requires complex checking that is not feasible with basic audit methods.

Not Applicable

This setting is a “policy”-style recommendation or general best practice that is not technical in nature.

1. Operating System and Network Specific Configuration

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
1.1	Physical security	Place the SQL Server in an area where it will be physically secure.	Place the server where only authorized personnel can obtain access.	1 N
1.2	Domain environment	If the SQL Server is in a domain that is trusted by other domains, document the access granted by the trust.	Ensure that the trusted domain has only the necessary rights to the SQL Server and its databases.	1 N
1.3	SQL Servers accessed via Internet	If the SQL Server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.	Limit the database contents of this SQL Server to information meant for public dissemination only.	1 N
1.4	SQL Servers accessed via Internet	Put a firewall between your server and the Internet. Block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too. In a multi-tier environment, use multiple firewalls to create more secure screened subnets.	Consider separating Web logic and business logic onto separate computers.	1 N
1.5	IPSEC	Use IPSEC policy filters to block connections to ports other than the configured SQL Server ports.	IPSEC offers authentication, integrity, confidentiality, and anti-replay services. SSL can provide these services for all database connections; however, IPSEC can allow these services to be configured on selected computers and ports.	2 S
1.6	Encryption	Implement SSL. Use the fully-qualified DNS name of the server in the certificate to help prevent masquerading.		2 S
1.7	Test and development servers	Maintain test and development servers on a separate network segment from the production servers.	Test patches carefully before applying them to production systems.	1 N
1.8	Dedicated Server	Install SQL Server on a computer that does not provide additional services, e.g., Web or Mail Services.	Vulnerabilities in other application services could lead to a compromise of the SQL Server.	1 N
1.9	OS Benchmark Configuration	Configure Windows 2003 Server Level I benchmark settings with the following modifications:		
1.9.1	Windows accounts	Make sure the Windows guest account is disabled		1 S
1.9.2	Disk subsystem	Use RAID for critical data files	Raid Level 10 is recommended. Use the level of RAID which will provide the best reliability and performance for your environment.	1 N

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
1.9.3	Separate partitions	Create separate partitions for OS/SQL program files, SQL data files, and SQL transaction logs.	Separate partitions provide greater protections via host and file permissions at the volume level as well as allowing greater control over data storage usage and monitoring of the database.	1 S
1.9.4	Volume / partition type	Format all volumes with NTFS		1 S
1.10	Services	Disable the following services on a SQL Server machine	The disabling of services has to be balanced with application requirements, since certain applications require the use of certain services to function correctly.	
1.10.1		Alerter		1 S
1.10.2		Clipbook Server		1 S
1.10.3		Computer Browser		1 S
1.10.4		DHCP Client		1 S
1.10.5		Distributed File System		1 S
1.10.6		Distributed Transaction Coordinator		2 S
1.10.7		Fax Service		1 S
1.10.8		Internet Connection Sharing		1 S
1.10.9		IPSec policy agent	Unless IPSec policies will be used	1 S
1.10.10		License Logging		1 S
1.10.11		Logical Disk Manager Administrative Service		1 S
1.10.12		Messenger		1 S
1.10.13		NetMeeting Remote Desktop Sharing		1 S
1.10.14		Network DDE		1 S
1.10.15		Network DDE DSDM		1 S
1.10.16		Print Spooler		1 S
1.10.17		Remote Access Connection Manager		1 S
1.10.18		Remote Registry	Unless network management software requiring remote registry access will be used	1 S
1.10.19		Removable Storage		1 S
1.10.20		RunAs Service		1 S
1.10.21		Smart Card		1 S
1.10.22		Smart Card Helper		1 S
1.10.23		Task Scheduler	Unless batch jobs scheduled with the SQL Server Agent or scheduled tasks will be used	1 S
1.10.24		Telephony		1 S
1.10.25		Telnet		1 S
1.10.26		Windows Installer		1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
1.11	MSSQL Server Service Account	Use a low-privileged Local or Domain account for the MSSQLServer service.	The services account should only be a domain account if the SQL Server requires remote communications with other domain systems such as those used for backup over the network. Otherwise, a local user account should be used. See items 1.13 – 1.17 for additional information on the service account.	2 N
1.12	SQLServerAgent Service Account	Use a low-privileged domain account for SQLServerAgent if replication, DTS, or other inter-server connection is required.	Replication and other inter-server communications require the SQLServerAgent service account to be a domain account.	1 N
1.13	Local users group membership	Assign the local service account as a member of only the Users group	The 'Users' group is a local machine group.	1 S
1.14	Domain users group membership	Make a domain service account a member of only the Domain Users group		1 N
1.15	SQL Server service account rights	Grant the SQL Server service account(s) the following rights:	These rights are assigned by default.	
		Log on as a service		1 S
		Act as part of the operating system		1 S
		Log on as a batch job		1 S
		Replace a process-level token		1 S
		Bypass traverse checking		1 S
		Adjust memory quotas for a process		1 S
		Permission to start SQL Server Active Directory Helper		1 S
		Permission to start SQL Writer		1 S
1.16	SQL Server Agent service account rights	Grant the SQL Server Agent service account(s) the following rights:	These rights are assigned by default.	
		Log on as a service		1 S
		Act as part of the operating system	Only on Windows 2000	1 S
		Log on as a batch job		1 S
		Replace a process-level token		1 S
		Bypass traverse checking		1 S
		Adjust memory quotas for a process		1 S
1.17	Integration Service account rights	Grant the Integration Service account(s) the following rights:		
		Log on as a service		1 S
		Permission to write to the application event log		1 S
		Bypass traverse checking		1 S
		Create global objects		1 S
		Impersonate a client after authentication		1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
1.18	SQL Server services account rights	Deny the service account the “Log on locally” right.	The service accounts do not have a need to log on to the console. This will prevent a brute force attack on the service account.	1 S
1.19	SQL Server services account rights	If a service account is a domain account, configure the account to have the Windows permission “Log on Locally” the database server only.	This, combined with the recommendation in item 1.15-1.17, will prevent an attempt to logon to any domain computer using the services account.	1 N
1.20.1	SQLServer Proxy accounts	Create dedicated user accounts specifically for proxies, and only use these proxy user accounts for running job steps.	A SQL Server Agent proxy defines the security context for a job step. A proxy provides SQL Server Agent with access to the security credentials for a Microsoft Windows user. Each proxy can be associated with one or more subsystems. A job step that uses the proxy can access the specified subsystems by using the security context of the Windows user. Before SQL Server Agent runs a job step that uses a proxy, SQL Server Agent impersonates the credentials defined in the proxy, and then runs the job step by using that security context.	1 N
1.20.2	SQLServer Proxy accounts	Only grant the necessary permissions to proxy user accounts. Grant only those permissions actually required to run the job steps that are assigned to a given proxy account.		1 N
1.20.3	SQLServer Proxy accounts	Do not run the SQL Server Agent service under a Microsoft Windows account that is a member of the Windows Administrators group.		1 S

2. SQL Server Installation and Patches

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
2.1	SQL Server install platform	Avoid installing SQL Server on a domain controller.	If SQL Server were installed on a domain controller, a successful attack against the database could potentially compromise all domain resources.	1 S
2.2	Patches and hotfixes	Ensure the Current SQL Server service pack and hotfixes are installed.	It would be counter productive to state specific patch levels and hotfixes in this document. Since they can change fairly often, the versions stated here might be outdated by the time this document is used. Check Microsoft's website for the latest service pack/hotfix for SQL Server 2005. Automatic updates are appropriate for non-production databases only. In multiple instance environments, updates must be applied to each SQL Server instance.	1 S
2.3	SQL Server Ports	Change SQL Server default ports from 1433 and 1434.	Using a non-default port helps protect the database from attacks directed to the default port.	1 S
2.4	Naming conventions	In naming SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Version or other sensitive information in the server name makes it easier for an attacker to develop an attack strategy against the server.	1 N
2.5	SQL Server instances	Keep an inventory of all versions, editions and languages of SQL Server.	Include instances of SQLEXPRESS. SQL Scan and SQL Check are some of the tools that can be used to scan for instances of SQL Server within a domain.	1 N
2.6	Authentication mode	Select Windows authentication mode.	Windows provides a more robust authentication mechanism than SQL Server authentication. If SQL Server authentication is required, configure SQL Server account password and lockout properties with local or domain-based group policies.	1 S
2.7	Rename sa account	The 'sa' account should be renamed to something that is not easily identifiable as the 'sa' account.	It is more difficult to script attacks against the 'sa' account if the username is not known.	1 S
2.8	Strong password	Use a strong password for the 'sa' login account.	A strong password for the "sa" login account is required regardless of which mode is chosen and regardless of whether the 'sa' account is disabled.	1 N

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
2.9	Sample databases	Do not install the sample databases. Delete all sample databases if they already exist.	e.g., AdventureWorks, AdventureWorksDW, Northwind and Pubs Note: None of the sample database are installed by default	1 S
2.10	Initialization parameter	C2 Audit Mode– Set to 1 if no custom defined audit trace is enabled	Specifies whether automatic auditing of security events is enabled.	1 S
2.11	Initialization parameter	Remote Access– Set to 0 unless replication is being used or the requirement is justified	Allows logons from remote servers.	1 S
2.12	Initialization parameter	Scan for Startup Procedures– Set to 0 unless justified	Sets SQL Server to scan for startup procedures when the service starts. Setting Scan for Startup Procedures to 0 will prevent audit traces and other commonly used monitoring SPs from re-starting on start up. This includes the MS-provided common criteria audit traceaudit which is included in the SQL Server 2005 EAL1 common criteria evaluation.See https://members.microsoft.com/sqlcommoncriteria/EAL1_trace.sql for additional details.	1 S

3. SQL Server Settings

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
3.1	SQL Server Configuration Manager	Disable the 'Named Pipes' network protocol.	If Named Pipes is required, change the name to something other than \\.\pipe\sql\query. Named Pipes protocol is disabled by default for MSSQLSERVER and SQLEXPRESS and enabled for SQL Native Client.	1 S
3.2	SQL Server Properties	The following settings are recommended:		
3.2.1	Auto Restart SQL Server	Set the SQL Server service start mode to 'Automatic'	This is found in the SQL Server Configuration Manager.	1 S
3.2.2	Auto Restart SQL Server Agent	If the SQL Server Agent is required, set the 'SQL Server Agent' start mode to 'Automatic'.	This is found in the SQL Server Configuration Manager.	1 S
3.2.3	Distributed Transaction Coordinator	Set the 'Distributed Transaction Coordinator' service start mode to 'Disabled' if this service is not required.	This is found in the SQL Server Configuration Manager.	1 S
3.2.4	Cross database-ownership chaining	Disable the cross_db_ownership_chaining option.	Use sp_dboption to check for databases for which cross-database ownership chaining is enabled. This is found in the General page of SQL Server Properties window. This is disabled by default.	1 S
3.2.5	Advanced Server Settings	Do not enable direct modifications to the system catalogs.	This access level is disabled by default in SQL Server 2005 and cannot be enabled. You must use the documented API's to access them.	1 S
3.2.6	Backup/Restore from tape timeout	Set the Backup/Restore from tape timeout period to "Try for 5 minutes"	This option is found in the Database Settings page of SQL Server Properties window.	1 S
3.2.7	Media Retention	Set the default backup media retention to the minimum number of days needed to retain a full backup of the database. Ideally, this should be as high as your resources permit.	This option is found in the Database Settings page of SQL Server Properties window.	1 N
3.3	Data Directory	The default data directory should be a dedicated data partition		1 S
3.4	Data Directory	The default log directory should be a dedicated partition separate from all programs and data		1 S
3.5	Replication	Do not enable replication.	Section 7 covers security recommendations if replication is required.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
3.6	Other SQL Server Configuration Options	Save a maximum of 14 SQL error logs.	Truncate logs on a regular schedule, weekly, bi-weekly etc. to prevent oversize logs. This option is found under Management-> SQL Server Logs ->Configure Note: The number of retained agents error logs cannot be customized as it is hard coded at nine.	1 S
3.7	Database Mail	Disable Database Mail where messaging is not required.	This option is found in the Advanced page of the SQL Server Properties window.	1 S
3.8	Trace Messages	Error Log/Include execution trace messages = off	General Page on SQL Server Agent properties	1 S
3.9	User-defined stored procedures	Ensure that all user-defined stored procedures are stored in encrypted format.		1 S
3.10	User-defined extended stored procedures	Avoid using user-defined extended stored procedures. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	This feature will be removed in a future version of SQL Server	1 S
3.11	Extended stored procedures	Disable access to the following extended stored procedures:	The disabling of access to stored procedures has to be balanced with application requirements, since certain applications require the use of external stored procedures to either export or import data. In the case where stored procedures need to be left on the server, document this information and note as an exception.	
3.11.1		xp_available media		2 S
3.11.2		xp_cmdshell	Disabled by default	1 S
3.11.3		xp_dirtree		2 S
3.11.4		xp_dsninfo		2 S
3.11.5		xp_enumdsn		2 S
3.11.6		xp_enumerrorlogs		2 S
3.11.7		xp_enumgroups		2 S
3.11.8		xp_eventlog		2 S
3.11.9		xp_fixeddrives		2 S
3.11.10		xp_getfiledetails		2 S
3.11.11		xp_getnetname		2 S
3.11.12		xp_logevent		2 S
3.11.13		xp_loginconfig		2 S
3.11.14		xp_msver		2 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
3.11.15		xp_readerrorlog		2 S
3.11.16		xp_servicecontrol		2 S
3.11.17		xp_sprintf		2 S
3.11.18		xp_sscanf		2 S
3.11.19		xp_subdirs		2 S
3.12	SQLmail extended stored procedures	Disable access to the following SQLMail extended stored procedures:	SQLMail is replaced by Database mail in MSS2005. It remains for backwards compatibility. Both mail tools are disabled by default.	
3.12.1		xp_deletemail	Disabled by default	2 S
3.12.2		xp_findnextmsg	Disabled by default	2 S
3.12.3		xp_get_mapi_default_profile	Disabled by default	2 S
3.12.4		xp_get_mapi_profiles	Disabled by default	2 S
3.12.5		xp_readmail	Disabled by default	2 S
3.12.6		xp_sendmail	Disabled by default	2 S
3.12.7		xp_startmail	Disabled by default	2 S
3.12.8		xp_stopmail	Disabled by default	2 S
3.13	WebTask extended stored procedures	Disable access to the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following Web Task extended stored procedures:	WebTask is disabled by default.	
3.13.1		xp_cleanupwebtask	Disabled by default.	2 S
3.13.2		xp_convertwebtask	Disabled by default.	2 S
3.13.3		xp_dropwebtask	Disabled by default.	2 S
3.13.4		xp_enumcodepages	Disabled by default.	2 S
3.13.5		xp_makewebtask	Disabled by default.	2 S
3.13.6		xp_readwebtask	Disabled by default.	2 S
3.13.7		xp_runwebtask	Disabled by default.	2 S
3.14	OLE Automation stored procedures	Disable access to the following OLE Automation stored procedures:	Disabled by default.	
3.14.1		sp_OACreate	Disabled by default	2 S
3.14.2		sp_OADestroy	Disabled by default	2 S
3.14.3		sp_OAGetErrorInfo	Disabled by default	2 S
3.14.4		sp_OAGetProperty	Disabled by default	2 S
3.14.5		sp_OAMethod	Disabled by default	2 S
3.14.6		sp_OASetProperty	Disabled by default	2 S
3.14.7		sp_OAStop	Disabled by default	2 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
3.15	Registry access extended stored procedures	Disable access to the following Registry access extended stored procedures:		
3.15.1		xp_regaddmultistring		2 S
3.15.2		xp_regdeletekey		2 S
3.15.3		xp_regdeletevalue		2 S
3.15.4		xp_regenumvalues		2 S
3.15.5		xp_regremovemultistring		2 S
3.15.6		xp_regwrite		2 S
3.16	Advanced Setting	SQL Server Event forwarding/Forward events to a different server = off	SQL Server Agent properties page.	1 S

4. Access Controls

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
4.1	Permissions on OS tools	Restrict access to the executables in the System32 directory eg. Explorer.exe and cmd.exe.	Remove the Users group's permission (if any) to executables. Assign Administrators Full Control.	1 S
4.2	SQL Server install directory permissions	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL Server directory.	Assign the SQL Server service account Full Control. Remove the Users group's permission.	1 S
4.3	SQL Server database instance directory permissions	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\Install, e.g., sqlstp.log, sqlsp.log and setup.iss. '.X' represents the installations of various SQL Server installs due to the fact that multiple instances of SQL Server or SQL Express can be installed.	If the current system was upgraded from SQL Server version 2000, check setup.iss in the %Windir% folder and the sqlstp.log in the Windows Temp folder for passwords. Microsoft distributes a free utility called Killpwd, which will locate and remove passwords found in these setup files from your system. This tool does not work with a native SQL 2005 installation. Microsoft is scheduled to release an updated tool, but no release date has been given at this time.	1 S
4.4	Assigning System Administrators role	When assigning database administrators to the System Administrators role, map their Windows accounts to SQL logins, then assign them to the role.	Assign only authorized DBAs to the SQL Server System Administrators role.	1 N
4.5	SQL Logins	Remove the default BUILTIN\Administrators SQL login.	Do not remove BUILTIN\Administrators until another account has been assigned the System Administrators role.	1 S
4.6	SQL Logins	Ensure that all SQL Logins have strong passwords.	Verify that the passwords are not blank and cannot be easily compromised.	1 N
4.7	OS Guests access	Deny database login for the Guests OS group.	Assuming your Guests group was not renamed as part of your OS lockdown: EXEC sp_denylogin 'Computer_Name\Guests'	1 S
4.8	Fixed Server Roles	Only use the fixed server roles sysadmin, serveradmin, setupadmin etc, to support DBA activity.	Avoid assigning these roles to application database user accounts, application administrator accounts, application developer accounts or application roles.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
4.9	SQL Server Database Users and Roles	Remove the guest user from all databases except master and tempdb.		1 S
4.10	Statement Permissions	Grant DDL statement permissions to only the database and schema owner, not individual users.	DBO has all statement permissions for the database by default	1 S
4.11	Database Owners Permissions	Ensure dbo owns all user-created database schemas	Having dbo own all user-created database schemas prevents issues raised when users need to be deleted	1 S
4.12	Low-privileged users	Do not grant object permissions to PUBLIC or GUEST.	Do not grant the REFERENCES object permission to an application user, application administrator, or application role.	1 S
4.13	Stored Procedure Permissions	Grant execute permissions on stored procedures to database roles (not users).		1 S
4.14	Using the GRANT option	Do not assign the GRANT option of object permission to a user or role.		1 S
4.15	SQL Server Agent subsystem privileges	Restrict proxy access to required/approved subsystems	Allowing access to CmdExec and ActiveX subsystems allows direct OS access and should be avoided unless business justifications for doing so exist.	1 N
4.16	User-defined Database Roles	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.	Not all organizations have a need for user-defined database roles. This may not apply to all organizations.	1 N
4.17	Database Roles	Avoid nesting database roles.		1 S
4.18	Users and Roles	Ensure that the members of the roles (users/groups/other roles) in the target database actually exist.		1 S
4.19	Application Roles	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string. Use “EXECUTE AS WITH NO REVERT” or “WITH COOKIE” to allow individuals to access the application without knowing the password.	This provides a permission based rather than password based mechanism to sandbox access.	1 N
4.20	Use of Predefined Roles	Avoid assigning predefined roles to PUBLIC or GUEST.		1 S
4.21	Linked or Remote Servers	Use linked servers rather than remote servers where required. Disable linked servers otherwise	Remote servers are available for backward compatibility purposes only. Applications that must execute stored procedures against remote instances of SQL Server should use linked servers instead.	1 S
4.22	Linked or Remote Servers	Configure linked or remote servers to use Windows authentication where required. Disable linked servers otherwise.	When linking SQL Server databases, the user’s current identity will be used to authenticate the connection.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
4.23	Linked Server logins	Allow linked server access only to those logins that need it. Disable linked servers otherwise.		1 N
4.24	Ad Hoc Data Access	Disable ad hoc data access on all providers except SQL OLE DB, for all users except members of the sysadmin fixed role. Use network segmentation to prevent or limit desktop clients from making direct adhoc connections.	Allow ad hoc data access only to trusted providers. Limit adhoc connections from MS Office applications (Excel, Access, Word, etc.).	1 N

5. Auditing and Logging

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
5.1	Auditing – General	Prepare a schedule for reviewing audit information regularly.		1 N
5.2	SQL Server Properties – Security Tab	Through the SQL Server Management Studio, enable auditing for SQL Server.	At a minimum, enable failed login attempts. Auditing of failed login attempts only is enabled by default.	1 S
5.3	SQL Server Logs	SQL Server audit data must be protected from loss. The SQL Server and SQL Server Agent logs must be backed up before they are overwritten.	Adjust the number of logs to prevent data loss. The default is six.	1 N
5.4	SQL Profiler	Use SQL Profiler to generate and manage audit trails.	Ensure sufficient resources to support Profiler activity	1 S
5.5	Profiler Events	Capture the following events using SQL Profiler	A third-party auditing tool may be used in lieu of SQL Profiler.	
		Event	**Description of what the event records**	
5.5.1		Audit Add DB User Event	Occurs when a database user login has been added or removed.	1 S
5.5.2		Audit Add Login to Server Role	Addition or removal of login accounts to/from server roles.	1 S
5.5.3		Audit Add Member to DB Role	Addition and deletion of logins from a database role.	1 S
5.5.4		Audit Add Role Event	Occurs when a database role is added or removed.	1 S
5.5.5		Audit Addlogin Event	Occurs when a login has been added or removed.	1 S
5.5.6		Audit App Role Change Password	Whenever passwords are changed for an application role.	1 S
5.5.7		Audit Backup/Restore	Occurs whenever a backup or restore command is issued.	1 S
5.5.8		Audit Broker Conversation	Reports audit messages related to Service Broker dialog security.	1 S
5.5.9		Audit Broker Login	Reports audit messages related to Service Broker transport security.	1 S
5.5.10		Audit Change Audit	Occurs whenever an audit trace modification is made.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
5.5.11		Audit Change Database Owner	Occurs when you use the ALTER AUTHORIZATION statement to change the owner of a database, and the permissions required to do that are checked.	1 S
5.5.12		Audit DBCC	Occurs whenever a DBCC command is issued	1 S
5.5.13		Audit Database Management	Occurs when a database is created, altered, or dropped.	1 S
5.5.14		Audit Database Object Access	Occurs when database objects, such as schemas, are accessed.	1 S
5.5.15		Audit Database Object GDR	Occurs when a GRANT, REVOKE, or DENY has been issued for database objects, such as assemblies and schemas.	1 S
5.5.16		Audit Database Object Management	Occurs when a CREATE, ALTER, or DROP statement is executed on database objects, such as schemas.	1 S
5.5.17		Audit Database Object Take Ownership	Occurs when a change of owner for objects within database scope occurs.	1 S
5.5.18		Audit Database Operation	Occurs when operations in a database, such as checkpoint or subscribe query notification, occur.	1 S
5.5.19		Audit Database Principal Impersonation	Occurs when an impersonation occurs within the database scope, such as EXECUTE AS <*user*> or SETUSER.	1 S
5.5.20		Audit Database Principal Management	Occurs when principals, such as users, are created, altered, or dropped from a database.	1 S
5.5.21		Audit Database Scope GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a statement permission by any user in Microsoft SQL Server for database-only actions such as granting permissions on a database.	1 S
5.5.22		Audit Login Change Password	Occurs whenever a user changes their Microsoft SQL Server login password.	1 S
5.5.23		Audit Login Change Property	Occurs when you use the sp_defaultdb stored procedure, the sp_defaultlanguage stored procedure, or the ALTER LOGIN statement to modify a property of a login.	1 S
5.5.24		Audit Login	Occurs when a user has successfully logged in to SQL Server.	1 S
5.5.25		Audit Login Failed	Indicates that a user tried to log in to Microsoft SQL Server and failed.	1 S
5.5.26		Audit Login GDR Event	Occurs when a Microsoft Windows login right was added or removed.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
5.5.27		Audit Logout	Indicates that a user has logged out of (logged off) Microsoft SQL Server.	1 S
5.5.28		Audit Object Derived Permission Event	Occurs when a CREATE, ALTER, or DROP was issued for an object.	1 S
5.5.29		Audit Schema Object Access	Occurs when an object permission (such as SELECT) is used.	1 S
5.5.30		Audit Schema Object GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a schema object permission by any user in Microsoft SQL Server.	1 S
5.5.31		Audit Schema Object Management	Occurs when server objects are created, altered, or dropped.	1 S
5.5.32		Audit Schema Object Take Ownership	Occurs when the permissions to change the owner of schema object (such as a table, procedure, or function) is checked. This happens when the ALTER AUTHORIZATION statement is used to assign an owner to an object.	1 S
5.5.33		Audit Server Alter Trace	Occurs for all statements that check for the ALTER TRACE permission. Statements that check for ALTER TRACE include those used to create or configure a trace, or to set a filter on a trace.	1 S
5.5.34		Audit Server Object GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a server object permission by any user in Microsoft SQL Server.	1 S
5.5.35		Audit Server Object Management	Occurs in the case of CREATE, ALTER, or DROP for server objects.	1 S
5.5.36		Audit Server Object Take Ownership	Occurs when the owner is changed for objects in server scope.	1 S
5.5.37		Audit Server Operation	Occurs when Security Audit operations such as altering settings, resources, external access, or authorization are used.	1 S
5.5.38		Audit Server Principal Impersonation	Occurs when there is an impersonation within server scope, such as EXECUTE AS <*login*>.	1 S
5.5.39		Audit Server Principal Management	Occurs when server principals are created, altered, or dropped.	1 S
5.5.40		Audit Server Scope GDR	Occurs when a GRANT, REVOKE, or DENY is issued for permissions in the server scope, such as creating a login.	1 S
5.5.41		Audit Server Starts and Stops	Occurs when the Microsoft SQL Server service state is modified.	1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
5.5.42		Audit Statement Permission Event	Occurs when a statement permission has been used.	1 S

6. Backup and Disaster Recovery Procedures

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
6.1	Backups – General	Use Full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Database backups should be made to another server or disk that is not physically attached to the same server as the database. This will reduce the risk of total loss in case of disk failure.	1 N
6.2	System databases	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	The tempdb database contains no permanent data and does not require backups.	1 N
6.3	Backing up Master database	Backup the master database when any of the following events occur: • A database is created or deleted • Login accounts are created, deleted or modified • Server-wide or database settings are modified		1 N
6.4	Backing up MSDB database	Backup the msdb database when any of the following events occur: • Alerts, jobs, schedules or operators are created, deleted or modified • Backups and restores are performed		1 N
6.5	Backup Media	Password protect the backup media.	Assign a password to backups to reduce the probability of an incorrect data restore. Note: This password is not intended to prevent unauthorized access to backup data. See http://msdn.microsoft.com/en-us/library/ms186865(SQL.90).aspx for additional details.	2 N
6.6	Access to Backup Files	Restrict access to the backup files to System Administrators.		1 S
6.7	Access to Backup Files	Restrict restore permissions to DBAs and db_owners.		1 S

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
6.8	Recommended periodic administrative procedures	Run the Microsoft Baseline Security Analyzer weekly and follow the security recommendations as closely as possible to secure the operating system.		1 N
6.9	Recommended periodic administrative procedures	Run the SQL Best Practices Analyzer regularly and note any changes to the environment.		1 N
6.10	Enable Password Policy Enforcement	When a password change mechanism is introduced into clients and applications, enable password expiration. Always specify MUST_CHANGE when specifying a password on behalf of another principal.		1 S
6.11	Periodic scan of Role Members	Periodically scan fixed server and database roles to ensure that only trusted individuals are members.		1 N
6.12	Periodic scan of stored procedures	Verify stored procedures that have been set to AutoStart are secure.		1 N

7. Replication

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
7.1	SQL Server Agent service account	Configure replication agents to use a Windows account rather than a SQL Server Agent account. Grant only the required permissions to each agent.	Use Windows Authentication for all replication agent connections.	1 S
7.2	Replication administration roles	Avoid modifying replication administration permissions assigned to the roles by default. Only assign authorized application administrators and DBAs these roles.	The permissions needed to support and administer replication are assigned to sysadmin, db_owner and replmonitor by default.	1 N
7.3	Snapshot share folder	Store the snapshot folder, which houses a snapshot of the replicated changes, on an explicit share and not an administrative share.		1 S
7.4	Publication Access List	The domain accounts used by the SQL Server Agent service and the Replication proxy account must be entered in the Publication Access List so that all replication agents will be able to participate in the replication process.		1 S
7.5	Secure Communications	Use secure connections, such as VPN or proxy servers, for all replication over the Internet.		1 N
7.6	Database connections	Configure the database connections for replication agents to use Windows authenticated logons.		1 S
7.7	Filtering	Employ replication filters to protect the data.		1 S
7.8	Distribution databases	All distribution databases and snapshot files must be located in protected and audited locations.		1 S

8. Application Development Best Practices

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
8.1	Ownership Chaining	Use ownership chaining within a single database to simplify permissions management.	Avoid using cross database ownership chaining.	1 N
8.2	Role Assignments	Assign permissions to roles rather than users. The principle of "Least Privilege" applies, thus users should not be given access to roles they do not need for their job function.	Ensure that roles, rather than users own objects to avoid application changes when a user is dropped.	1 N
8.3	Encrypted connections	Enable encrypted connections between the user and the server.	Consider allowing only encrypted connections. When allowing SQL Server authentication, encrypt either the network layer with IPSec or the session with SSL	1 N
8.4	Error Handling	Do not propagate errors back to the user.	Log errors or transmit them to the system administrator.	1 N
8.5	User Input	Prevent SQL injection by validating all user input before transmitting it to the server.	Only permit minimally privileged accounts to send user input to the server. Minimize the risk of SQL injection attack by using parameterized commands and stored procedures.	1 N
8.6	Developer awareness	Increase awareness of issues such as cross-site scripting, buffer overflows, SQL injection and dangerous APIs.		1 N
8.7	Developer awareness	Identify categories of threats that apply to your application, such as denial of service, escalation of privileges, spoofing, data tampering, information disclosure and repudiation.		1 N
8.8	Security reviews	Add security reviews to all stages of the application development lifecycle (from design to testing).		1 N
8.9	Distributing SQLEXPRESS	If you distribute SQLEXPRESS, install SQLEXPRESS using Windows security mode as the default.	Never install a blank sa password. Use the Microsoft Installer to install SQLEXPRESS.	1 N
8.10	Net-Libraries	If SQLEXPRESS will operate as a local data store, disable any unnecessary client protocols.	Remote access is disabled by default.	1 N

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
8.11	Customer awareness	Let your customers know that your product includes SQLEXPRESS so that they can be prepared to install or accept SQLEXPRESS -specific software updates.		1 N
8.12	SQL Server Agent	Change the SQL Server Agent Startup Type to “Disabled”.	SQLEXPRESS installs SQL Server Agent by default and the Service startup type is “Manual”.	1 N

9. Surface Area Configuration Tool

Item #	Configuration Item	Action / Recommended Parameters	Comments	Levels
9.1	Ad Hoc Remote Queries	Disable Ad Hoc Remote Queries where not required	Disabled by default.	1 S
9.2	CLR Integration	Disable CLR Integration where not required	Disabled by default.	1 S
9.3	DAC	Disable the Dedicated Administrator Connection where not required	Disabled by default.	1 S
9.4	Database Mail	Disable Database Mail where messaging is not required	Disabled by default.	1 S
9.5	Native XML Web Services	Do not configure XML Web Services endpoints where not required	Disabled by default.	1 S
9.6	OLE Automation	Disable OLE Automation where not required	Disabled by default.	1 S
9.7	Service Broker	Do not configure Service Broker endpoints where not required	Disabled by default.	1 S
9.8	SQL Mail	Do not enable SQL Mail where not required or where Database Mail could be used instead.	Disabled by default.	1 S
9.9	Web Assistant	Disable Web Assistant where not required	Disabled by default.	1 S
9.10	xp_cmdshell	Disable the xp_cmdshell stored procedure where not required	Disabled by default.	1 S
9.11	Ad Hoc Data Mining	Disable ad hoc data mining queries where not required		1 S
9.12	Anonymous Connections	Disable anonymous connections to the Analysis Services where not required		1 S
9.13	Linked Objects	” Enable links To other instances” should be disabled where not required.		1 S
9.14	Linked Objects	” Enable links From other instances” should be disabled where not required.		1 S
9.15	User-Defined Functions	Disable loading of user-defined COM functions where not required		1 S
9.16	Scheduled Events and Report Delivery	Disable scheduled events and report delivery where not required		1 S
9.17	Web Service and HTTP Access	Disable Web Service and HTTP access where not required		1 S
9.18	Windows Integrated Security	Enable Windows integrated security for report data source connections		1 S

Change History

Date	Version	Changes for this version
December 5th , 2008	1.1.0	• Updated TOU and Cover Page • Added Change History • Added Acknowledgements Section • Reformatted References Section • Removed 2.10 which recommended deleting regedit.exe. • 2.3 - Removed "Use host and/or network firewalls to help prevent attacks that target SQL Server on any port" from Comments section • 1.4 Added "Block TCP port 1433 and UDP port 1434 on your perimeter firewall. If named instances are listening on additional ports, block those too" to Action section. • Updated 2.12 (was 2.13) to note "'Setting Scan for Startup Procedures to 0' will prevent audit traces and other commonly used monitoring sps from re-starting on start up. This includes the MS-provided common criteria audit traceaudit trace is/was included in the SQL Server 2005 EAL1 common criteria evaluation. https://members.microsoft.com/sqlcommoncriteria/EAL1_trace.sql" • Remove item 3.6 as it was duplicative of 2.12 (then 2.13) • Updated 2.9 to note "None of the sample database are installed by default". • Updated 3.14 to note "Disabled by default". • Updated 3.12 to note "SQLMail is replaced by Database mail in MSS2005. It remains for backwards compatibility. Both mail tools are disabled by default." • Added note to 3.6 which states "The number of retained agents error logs cannot be customized as it is hard coded at nine." • Updated 6.5 to level 2. Updated description to note that this password is not meant to prevent unauthorized access to backup data but to reduce the probability of restoring the incorrect dataset. • Set 3.11.2 (xp_cmdshell) as Level 2 and denoted that it is disabled by default. • Updated 3.12.x (SQLMail XPs) to note these items are disabled by default. • Updated 3.13.x (WebTask XPs) to note these items are disabled by default. • Updated 3.14.x (OLE Automation SPs) to note these items are disabled by default. • Removed item 6.6 which recommended against performing network backups. Updated subsequent numbering. • Adding Scoring Status information to each recommendation

Acknowledgements

The following people were instrumental in the development of this guide:

- Michael Fowkes
- Phyllis R. Palmer
- Rajendra Modak
- Mike Chapple
- Jitesh Chanchani
- Balaji Devarasetty
- Sheila Christman
- Ernesto Rojas
- James Hayes
- Drew Miners
- Tyler Harding
- Michael Anderson
- Brian Lawton
- Michael Mychalczuk
- Blake Frantz
- Al Comeau
- Dana Hemlock
- Paul Davis
- David W. Blaine
- Dave Shackleford
- Tran Thanh Chien
- Michael A. Davis
- Alexey Stolpovskikh
- John Thorpe
- William Edmond Jr.
- John Banghart
- Carl Alcindor
- Andrea J. Weber
- Jannine Mahone

References

- 10 Steps to Help Secure SQL Server 2000. Microsoft Corporation. Last accessed at: http://www.microsoft.com/sql/techinfo/administration /2000/security/securingsqlserver.mspx

- Database Security Technical Implementation Guide version 7, release1, October 2004. Developed by DISA for the DOD.

- Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000. August 26, 2003. National Security Agency.

- SQL Server 2000 SP3 Security Features and Best Practices: Security Best Practices Checklist. May 2003. Microsoft Corporation. Last accessed at:

  http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec04.mspx

- SQL Server Security Checklist. Last accessed at: http://www.securitymap.net/sdm/docs/windows/mssql-checklist.html

- SQL Server 2005 Security and Protection. Last accessed at: http://www.microsoft.com/technet/prodtechnol/sql/2005/library/security.mspx

- Microsoft MSDN Website Documentation:
  1. http://msdn2.microsoft.com/en-us/library/ms186515.aspx
  2. http://msdn2.microsoft.com/en-us/library/ms151227.aspx
  3. http://msdn2.microsoft.com/en-us/library/ms151219.aspx
  4. http://msdn2.microsoft.com/en-us/library/ms151775.aspx
  5. http://msdn2.microsoft.com/en-us/library/ms151772.aspx
  6. http://msdn2.microsoft.com/en-us/library/ms187892.aspx
  7. http://msdn2.microsoft.com/en-US/library/ms175537.aspx
  8. http://msdn2.microsoft.com/en-us/library/ms179313.aspx
  9. http://msdn2.microsoft.com/en-us/library/ms191148.aspx