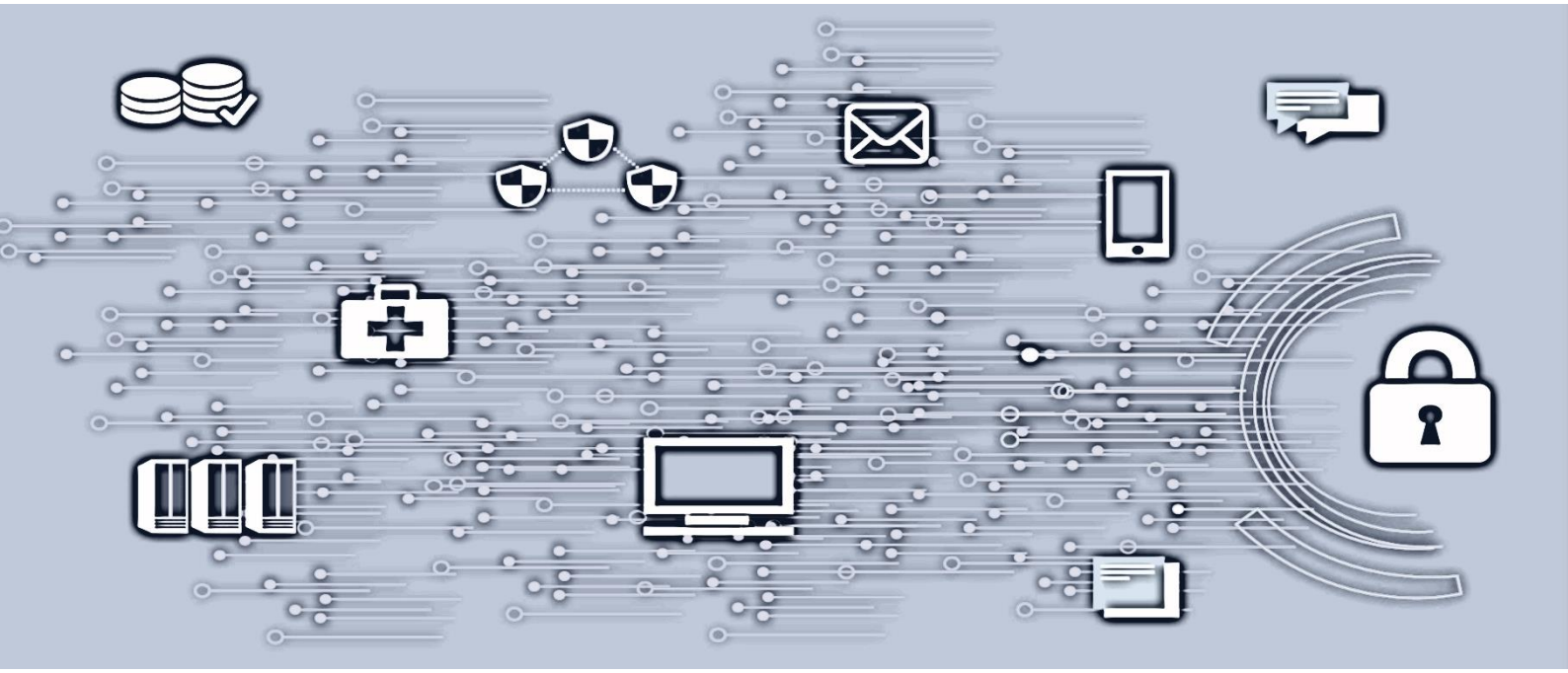
SYKEHUSPARTNER

Sikring av MSSQL-databaser



Innhold

Versjon	Dato	Godkjent av
1.1	2022-12-14	Christian Jacobsen

1. Hvordan bruke dokumentet

Databaser som innføres i Sykehuspartner skal følge standarden som er bestemt av Sykehuspartners Databasegruppe, dette er sikkerhetstiltak for å minske angrepsflaten på en MSSQL-server.

Hvis applikasjon/database ikke støtter mekanismene under, skal det skrives en forklaring på hvorfor.

Det er leverandør av systemet/databasen som skal uttale seg om reglene/innstillingene nedenfor. Reglene/innstillingene er standard satt ved oppsett av en MSSQL-server/MSSQL-database, avvik fra standarden må dokumenteres og godkjennes.

Det er leverandøren av systemet/databasen som skal fylle ut skjema. Skjema er derfor utarbeidet på engelsk.

2. Unntak fra sikkerhetsprinsippene

Unntak fra sikkerhetsprinsippene skal dokumenteres i risikovurderingen av løsningen.

3. MSSQL database

This chapter is relevant for all applications using MSSQL.

Settings	Supported Yes/No	Explain if No
Confirm that these Server settings are ok for the Database. (Vendors with SYSADMIN)		
Vendor's will normally not get SYSADMIN rights, can be given for short period under installation or for support		
'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'		
'CLR Enabled' Server Configuration Option is set to '0'		
'Cross DB Ownership Chaining' Server Configuration Option is set to '0'		
'Ole Automation Procedures' Server Configuration Option is set to '0'		
'sa' Login Account is set to 'Disabled'		
'xp_cmdshell' Server Configuration Option is set to '0'		
'Server Authentication' Property is set to 'Windows Authentication Mode'		
Confirm that these Database settings are ok for the Database. (Vendors with/without SYSADMIN)		
'Orphaned Users' are Dropped From SQL Server Databases		
Database default file location for all user databases, according to Sykehuspartner's standard: Data: E:\MSSQLUserDB\ Log: F:\MSSQLUserLog\		
State that the application user, do not need higher right's than DB_OWNER		
Regarding upgrade of the Application/database, state that there are no need for use of SA or members of SYSADMIN role		
Audit on SQL Engine will be Enabled, not on database level		

3.1 Patching of system:

The system must follow Sykehuspartner HF patch routines. Critical patches and security patches must be installed according to Sykehuspartner HF overall patch routines. Patches must be installed according to Common Vulnerability Scoring System (CVSS).

CVSS Score table:

Rating	CVSS score	Time to implement patch:
Low	0,1 - 3,9	30 work days
Medium	4,0 - 6,9	30 work days
High	7,0 - 8,9	12 work days
Critical	9,0 - 10,0	48 hours

3.2 Policy explanation:

Regel	Forklaring
'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'	**Description:** Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This functionality should be disabled. **Rationale:** This feature can be used to remotely access and exploit vulnerabilities on remote SQL Server instances and to run unsafe Visual Basic for Application functions.
'CLR Enabled' Server Configuration Option is set to '0'	**Description:** The `clr enabled` option specifies whether user assemblies can be run by SQL Server. **Rationale:** Enabling use of CLR assemblies widens the attack surface of SQL Server and puts it at risk from both inadvertent and malicious assemblies.
'Cross DB Ownership Chaining' Server Configuration Option is set to '0'	**Description:** The `cross db ownership chaining` option controls cross-database ownership chaining across all databases at the instance (or server) level. **Rationale:** When enabled, this option allows a member of the `db_owner` role in a database to gain access to objects owned by a login in any other database, causing an unnecessary information disclosure. When required, cross-database ownership chaining should only be enabled for the specific databases requiring it instead of at the instance level for all databases by using the `ALTER DATABASE <database_name> SET DB_CHAINING ON` command. This database option may not be changed on the `master`, `model`, or `tempdb` system databases.
'Ole Automation Procedures' Server Configuration Option is set to '0'	**Description:** The `Ole Automation Procedures` option controls whether OLE Automation objects can be instantiated within Transact-SQL batches. These are extended stored procedures that allow SQL Server users to execute functions external to SQL Server. **Rationale:** Enabling this option will increase the attack surface of SQL Server and allow users to execute functions in the security context of SQL Server.
'sa' Login Account is set to 'Disabled'	**Description:** The `sa` account is a widely known and often widely used SQL Server account with sysadmin privileges. This is the original login created during installation and always has the `principal_id=1` and `sid=0x01`. **Rationale:** Enforcing this control reduces the probability of an attacker executing brute force attacks against a well-known principal.
'xp_cmdshell' Server Configuration Option is set to '0'	**Description:** The `xp_cmdshell` option controls whether the `xp_cmdshell` extended stored procedure can be used by an authenticated SQL Server user to execute operating-system command shell commands and return results as rows within the SQL client. **Rationale:** The `xp_cmdshell` procedure is commonly used by attackers to read or write data to/from the underlying Operating System of a database server.
'Server Authentication' Property is set to 'Windows Authentication Mode'	**Description:** Uses **Windows Authentication** to validate attempted connections. **Rationale:** Windows provides a more robust authentication mechanism than SQL Server authentication.

'Orphaned Users' are Dropped From SQL Server Databases	**Description:** A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance and is referred to as orphaned and should be removed. **Rationale:** Orphan users should be removed to avoid potential misuse of those broken users in any way.
Database default file location for all user databases, according to Sykehuspartner's standard: Data: E:\MSSQLUserDB\ Log: F:\MSSQLUserLog\	**Description:** This is the standard for Sykehuspartner where the database and log file are be placed. Database files and Log files, must use those paths. The disk's here are formatted with 64KB allocation unit size, optimized for SQL. **Rationale:** This gives SQL better performance and database file and log file are on separated disk's.
State that the application user, do not need higher right's than DB_OWNER	**Description:** This is the highest right needed for the application, there should not be any other user with higher then DBO for the application. **Rationale:** Users with db_owner role in a database, have full control over the database. And this user should be an administrator or Super User. This db_owner should not be the main user for the application, that should be a user with DB write/read.
Regarding upgrade of the Application/database, state that there are no need for use of SA or members of SYSADMIN role	**Description:** It should not be necessary to use a user with SA right's to do upgrade. **Rationale:** When upgrading the database, there is no need to use system Procedures or any other system related query's. So the user used for upgrade, only need db_owner right's.

Annet

Fyll inn annen relevant informasjon om systemet/tjenesten: