8.4 Privileged User Access

8.4 Ensure privileged user access events are logged

Description:

Log events of creation, modification and deletion on user/system accounts made by the privileged user role.

Rationale:

A privileged user, by definition, is a user who, by virtue of function, and or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users.

For instance the sysadmin (*sa*) role is the highest privilege with in an instances of SQL service, members of this role can make any changes to the system without contest. Actions of a privileged user MUST be recorded to provide a consistent audit of what is changed, when, and by whom.

Audit:

```
SELECT
 S.name AS 'Audit Name'
 , CASE S.is_state_enabled
 WHEN 1 THEN 'Y'
 WHEN 0 THEN 'N' END AS 'Audit Enabled'
 , S.type_desc AS 'Write Location'
 , SA.name AS 'Audit Specification Name'
 , CASE SA.is_state_enabled
 WHEN 1 THEN 'Y'
 WHEN 0 THEN 'N' END AS 'Audit Specification Enabled'
 , SAD.audit_action_name
 , SAD.audited_result
 FROM sys.server_audit_specification_details AS SAD
 JOIN sys.server_audit_specifications AS SA
 ON SAD.server_specification_id = SA.server_specification_id
 JOIN sys.server_audits AS S
 ON SA.audit_guid = S.audit_guid
 WHERE SAD.audit_action_id IN ('ADSP', 'CNAU', 'GRO', 'GRSV', 'MNSP',
'PWCG', 'TOSO');
```

The result set should contain 7 rows, one for each of the following audit_action_names:

- AUDIT_CHANGE_GROUP
- LOGIN_CHANGE_PASSWORD_GROUP
- SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP
- SERVER_OBJECT_PERMISSION_CHANGE_GROUP
- SERVER_PERMISSION_CHANGE_GROUP
- SERVER_PRINCIPAL_CHANGE_GROUP
- SERVER_ROLE_MEMBER_CHANGE_GROUP

Both the Audit and Audit specification should be enabled and the audited_result should include both success and failure.

Remediation:

Via the SSMS GUI Interface:

1. Expand the **SQL Server** in **Object Explorer**.
2. Expand the **Security Folder**
3. Right-click on the **Audits** folder and choose **New Audit...**
4. Specify a name for the **Server Audit**.
5. Specify the audit destination details and then click **OK** to save the **Server Audit**.
6. Right-click on **Server Audit Specifications** and choose **New Server Audit Specification...**
7. Name the **Server Audit Specification**
8. Select the just created **Server Audit** in the **Audit** drop-down selection.
9. Click the drop-down under **Audit Action Type** and select AUDIT_CHANGE_GROUP.
10. Click the new drop-down under **Audit Action Type** and select LOGIN_CHANGE_PASSWORD_GROUP.

Status APPLIED

Control:

This configuration is applied through the template build and divided into server and database privileged user audits, see the definition of these audits under Privileged User Access Audit Specification. To apply these controls execute the following scripts: config_cntl_8.4s, and config_cntl_8.4d.

11. Click the new drop-down under **Audit Action Type** and select SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP.
12. Click the new drop-down under **Audit Action Type** and select SERVER_OBJECT_PERMISSION_CHANGE_GROUP.
13. Click the new drop-down under **Audit Action Type** and select SERVER_PERMISSION_CHANGE_GROUP
14. Click the new drop-down under **Audit Action Type** and select SERVER_PRINCIPAL_CHANGE_GROUP.
15. Click the new drop-down under **Audit Action Type** and select SERVER_ROLE_MEMBER_CHANGE_GROUP.
16. Click OK to save the **Server Audit Specification**.
17. Right-click on the new **Server Audit Specification** and select **Enable Server Audit Specification**.
18. Right-click on the new **Server Audit** and select **Enable Server Audit**.

Via T-SQL

Execute code similar to:

```
CREATE SERVER AUDIT TrackPrivilegedUse
TO APPLICATION_LOG;
GO
CREATE SERVER AUDIT SPECIFICATION TrackAllServerPrivilegedUse
FOR SERVER AUDIT TrackPrivilegedUse
ADD (AUDIT_CHANGE_GROUP),
ADD (LOGIN_CHANGE_PASSWORD_GROUP),
ADD (SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SERVER_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (SERVER_PERMISSION_CHANGE_GROUP),
ADD (SERVER_PRINCIPAL_CHANGE_GROUP),
ADD (SERVER_ROLE_MEMBER_CHANGE_GROUP)
WITH (STATE = ON);
GO
ALTER SERVER AUDIT TrackPrivilegedUse
WITH (STATE = ON);
```

Note:

If the write destination for the Audit object is to be the security event log, see the Books Online topic Write SQL Server Audit Events to the Security Log and follow the appropriate steps.

Default Value:

By default, there are no audit object tracking login events.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/create-a-server-audit-and-server-audit-specification

back to Additional Considerations