Security requirement

M365 Power BI

Deutsche Telekom Group

Version	17 (internal)
Date	Nov 23, 2023
Status	In work

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	8.01	Security requirement

Version	State	Status
17 (internal)	Nov 23, 2023	In work

Contact	Validity	Released by
Telekom Security psa.telekom.de		

Summary
Power BI is a collection of software services, apps, and data connectors that work together to transform disconnected data sources into coherent, visually compelling, and interactive insights. The data can exist as an Excel spreadsheet or as a hybrid collection of cloud-based and on-premises data warehouse instances. With Power BI, it's possible to connect your data sources, discover and visualize key points, and share the results with relevant people.

Table of Contents

1. Introduction

This document was prepared on the basis of the requirements of the Group Security Policy. The present safety requirement serves, among other things, as a basis for approval in the PSA process. It also serves as an implementation recommendation for the requirements of the Group Security Policy in units that do not participate in the PSA procedure. These requirements must be taken into account during the planning and decision-making processes and apply to all M365 environments of the respective unit.

When implementing the security requirement, the priority national, international and supranational law must be observed. If compliance with the described requirements cannot be implemented or can only be implemented to a limited extent in individual cases, a risk assessment must be carried out together with a security and/or data protection expert (in accordance with the relevant requirement) and possible alternative protective measures must be coordinated.

2. Dataflow

Req 1	When using Power BI dataflows, the Viewer/Display workspace role should not be used

It is important to ensure that only report developers have direct access to a workspace containing Power BI dataflows. The "Viewer" / "Display" workspace role should not be used.
Separate workspaces must be used for Power BI dataflows and reports.

Motivation: All users who have the "Viewer" / "Display" role in a workspace are able to access all Power BI dataflows in the workspace via the Power BI Desktop Client (Cloud and Report Server Version). You can create and distribute your own reports based on dataflow data without the dataflow owner knowing. This requirement is intended to prevent this.

ID: 8.01-1/i17

Req 2	The Power BI Dataflow function “AutoML” (Automated Machine Learning) cannot be used.

AutoML (Automated Machine Learning) functionality is not permitted when creating and using a Power BI dataflow.
It must also be documented in the system description that this functionality will not be used.

Motivation: Until a final regulation has been made within the DTAG group for the handling of AI/AI and ML services, this requirement is intended to prevent the processing / manipulation of DTAG information by 3rd party services.

ID: 8.01-2/i17

3. Data Gateway

Req 3	Initiation of the connection must only be done from internal to external

Due to the very difficult to control data streams from external to internal, connections may only be established from internal to external. In this context, Intern is defined as On Premise or IaaS in a landing zone or private/public cloud controlled by your own organization. External, on the other hand, refers to the other areas of a public cloud or general resources on the Internet.

Validity: Application operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.01-3/i17

Req 4	The 4-eye principle when registering a data gateway in the tenant must be maintained

The right to register a data gateway in the desired tenant must be limited to a few employees. In order to comply with the 4-eyes principle, employees who have implemented or operate a data gateway must not be granted the right to register the data gateway in the tenant.

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.01-4/i17

Req 5	Permission level of the users of the data gateway must be set to "Can use"

A data gateway may be used but not shared with other users or applications. For this reason, the permission level for accounts that are authorized to the Data Gateway must be set to "Can use".

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.01-5/i17

Req 6	Every data gateway must be subject to a lifecycle process and management

The following lifecycle and management processes for a data gateway must be adhered to:

- Documentation of registering a data gateway in the tenant
- Purpose limitation of the data gateway; Documentation of the purpose limitation is carried out by the business case
- The data gateway must be managed centrally through platform operation

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 8.01-6/i17

4. Data Connectivity

Req 7	A disclaimer must be displayed when using import mode

When using Import Mode, a disclaimer must be displayed that informs users that using Import Mode uploads data from the data source to the cloud and stores it there.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Denial of executed activities

For this requirement the following warranty objectives are relevant:

ID: 8.01-7/i17

Req 8	When using Direct Query/Live Connect, an approval process must be implemented

An approval process must be implemented, released and used that allows or denies access to the data of the respective data source upon request. This must be documented in a user agreement between platform and application operation.

Validity: Platform operation

ID: 8.01-8/i17

Req 9	When using Data Flow, potential data from a source must be prevented from being displayed in a different form and/or from leaving the company boundaries.

When using Data Flow, the use and design must be specifically described and released, since it is possible using Data Flow to add data from a source in a modified form. The data owner is not automatically informed of this. In this context, a dedicated check must be carried out to determine whether this type of use has been approved by the data owner.

Validity: application operation

Motivation: Prevention of unwanted leakage of confidential information/data beyond company boundaries, as well as incorrect use of information/data that does not correspond to the classified data classification

ID: 8.01-9/i17

5. Reports

Req 10	Reports must be provided with a Default Sensitivity Label

If reports are created with Power BI, they must be provided with a sensitivity label from Microsoft Information Protection (MIP), which by default only allows employees of your own organization access to the respective report.

Validity: Application operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.01-10/i17

Req 11	A user agreement between the data owner and the consumer of a report must be concluded

The consumers of each report must be made aware of the correct handling of the data contained in the report. This can be realized by the data owner in several ways:

- User Agreement between Data Owner and Consumer
- Disclaimer in the Power BI workspace
- In the preamble to the report

Validity: Application operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 8.01-11/i17

Req 12	Users must not access an application's dataset with "Build-Permission" rights

To prevent users who do not have access to the workspace of an application or only a viewer role from accessing the dataset of an application and thus creating reports, the option "Allow all users to connect to the app's underlying datasets using the Build permission" must be deactivated at the Power BI app level or set to "Access to specific individuals or groups".

Validity: Application operation

Motivation: Minimization of the attack surface

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 8.01-12/i17

6. M365 General Requirements

6.1. Tenant & IAM

Req 13	Modern Authentication must be enabled

To prevent weak authentication from being used to log in to at least the following services, Modern Authentication must be enabled in the M365 Tenant:

- Exchange Online
- Skype for Business
- Sharepoint Applications

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-1/1.2

Req 14	Conditional Access (CA) must be used to prevent the use of legacy authentication

In order to prevent the use of weak authentication, so-called legacy authentication, a login that uses legacy authentication must be blocked by a suitable Condidtional Access Policy.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-2/1.2

Req 15	Multi Factor Authentication (MFA) must be enabled for each account using Conditional Access (CA)

To prevent the takeover of an account, e.g. through a password leak, every account that logs in to Azure Active Directory (AAD) via the Internet must use Multi Factor Authentication (MFA).

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system

- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-3/1.2

Req 16	Password Protection for Active Directory must be enabled

To prevent the use of weak or leaked passwords, Password Protection for Active Directory must be activated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 8.00-4/1.2

Req 17	A password reset of a privileged or break-glass account must be alerted

In order to check whether the change of password of a privileged or a break-glass account was lawful, any change of password of these accounts must be alerted.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-5/1.2

Req 18	Access to the Azure portal must be regulated according to the need-to-know or least-privilege principle

Access to the Azure portal may only be performed by some employees in compliance with the principles of need-to-know and least-privilege.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system

- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-6/1.2

Req 19	Only Privileged Access Workstations (PAW) may be used for privileged access to the tenant

To prevent privileged account compromise, privileged access to the M365 Tenant may only be performed using Privileged Access Workstations (PAW). The PAW shall meet at least the following requirements:

- Use of a modern endpoint detection and response solution such as Microsoft Defender for Endpoint or comparable
- The PAW must not have direct contact with the Internet, access to the M365 environment must be carried out via a separate infrastructure for privileged access
- The PAW must be particularly hardened and encrypted
- Authentication at the PAW must be done using MFA
- The user must not have local administration permissions on the PAW

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-7/1.2

Req 20	To document the privileged roles and authorizations used, an administration concept must be created

An administration concept must be created to document and trace the privileged roles and authorizations used within the M365 environment.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-8/1.2

Req 21	To protect identities, Microsoft Defender for Identity must be used

Microsoft Defender for Identity must be used to secure identities and detect abuse.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-9/1.2

Req 22	Defender for Cloud apps must leverage access controls and geo-blocking rules for privileged accounts

Microsoft Defender for Cloud Apps includes risk-based rules that detect unusual behavior or illogical actions. For example, if one authentication is made from one country and immediately afterwards a second one from an IP address of another country, it becomes visible within such a short period of time that this is logically not possible at all.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-10/1.2

Req 23	Cloud Service Provider (CSP) Administrative rights may not be used

Third parties (outside the platform operation) may not be granted CSP-delegated administration rights. Instead, a complete user account for the third party must be set up for such use cases, as this allows admin privileges to be assigned granularly.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-11/1.2

Req 24	Applications that use M365 services must be explicitly registered in the tenant

Applications that use M365 services must be explicitly registered in the tenant. Documentation, e.g. in the form of an interface agreement, must be prepared and signed.

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-12/1.2

6.2. Backend

Req 25	Every server that offers backend services for the M365 environment must be protected with a modern endpoint detection and response solution

Every server that offers backend services for the M365 environment must be protected with a modern endpoint detection and response solution, such as Microsoft Defender for Endpoint or similar

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-13/1.2

Req 26	A suitable centralized Mobile Device Management (MDM) solution must be used to access the M365 services

A suitable centralized Mobile Device Management (MDM) solution must be used to access the M365 services. A current OS level of the mobile device as well as a separation between private and business data as well as applications must be observed.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-14/1.2

6.3. Applications

Req 27	All applications that connect to M365 Services must use Web Account Manager (WAM)

All applications that connect to M365 Services must use Web Account Manager (WAM).

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-15/1.2

Req 28	Only shared third-party apps, addons, bots, connectors, etc. may be installed and used by the user

For example, to prevent unnoticed data exfiltration from the tenant, only centrally released third-party apps, addons, bots, connectors, etc. be installed and used by the user.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-16/1.2

Req 29	The Admin-Consent Workflow must be activated

To prevent a normal user from granting access permissions from or to an application, the admin consent workflow must be configured and activated accordingly.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-17/1.2

6.4. Data Security

Req 30	Links for External Sharing with Anonymous Access must be timed

To make data exfiltration by an attacker more difficult, external sharing links that allow anonymous access must be limited in time.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 8.00-18/1.2

Req 31	Data Loss Prevention Policies (DLP) must be configured and implemented

To prevent data leakage, for example in the context of an attack by hackers or by inattention, Data Loss Prevention Policies (DLP) must be implemented at the client level in the context of the respective application as well as at the platform level where this is technically possible.

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 8.00-19/1.2

Req 32	Microsoft Information Protection (MIP) must be configured and implemented

To protect the data to be processed and stored in the M365, Microsoft Information Protection must be implemented at the client level in the context of the respective application as well as at the platform level, where this is technically possible according to the current state.

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 8.00-20/1.2

Req 33	Custer Lockbox must be used

The Customer Lockbox feature must be used to protect the organization's data to be processed and stored in the M365 vis-à-vis the provider and the traceability of access to the organization's data by employees of the provider.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-21/1.2