iLink Digital

Microsoft Power BI Security Best Practices

Power BI by Microsoft lets users create self-service datasets, reports, dashboards, and visualizations with ease and speed. Using the Power BI service, you can connect to different data sources, combine data from those sources, and create shareable reports and dashboards.

Microsoft Power BI Software as Service runs on the Azure cloud computing platform.
It is currently deployed in numerous data centers across the world, serving customers in different regions. There is also an equal number of backups for each deployment.

The SaaS solution uses the Azure Active Directory (AAD) for customer authentication and management. It also leverages the Azure Traffic Manager (ATM) for directing traffic to the proximate data centers, based on the DNS record of the client.

Power BI Security Concerns

For many organizations, the security concerns with Power BI include the following questions:

- Who has access privileges to my data on the cloud?
- What if my data and reports get shared externally?
- Who can create workspaces and export data?
- Does a hybrid cloud expose my Power Bi datacenter?

Power BI Cloud Security Best Practices

User Authentication

The authentication process in Power Bi is governed by Azure Active Directory (AAD). The SaaS uses the customer's login credentials to grant access to the resource. You log into Power BI using the email address used to create your Power BI account.

Power BI then uses your login email as a username, passing it to resources whenever you attempt to connect to data sources. The username is mapped to UPN and resolved with a windows domain account for authentication.

You can use the Azure AD Conditional Access to attain additional layers of security when it comes to access authentication. You can also implement best practices, including:

- Multi-factor authentication (MFA) — turn this ON on Azure AD Conditional Access
- Blocking access from certain Operating Systems
- Restricting user accesses from untrusted locations
- Restricting access from individual clients using mobile

Data and Service Security

Power BI has robust encryption for both data at rest and data in transit. Data at rest is encrypted in Azure Blob Storage and Azure SQL DB. Data in transit is encrypted with HTTPs, while data in use is cached, encrypted, and stored in the Azure SQL database.

However, you are responsible for the data you share. You can access your data sources using your credentials, then share reports with a non-authenticated person. That is where Power BI security concerns arise. To bolster your Power BI data security, consider:

- Disabling the 'Share content with external users' setting on the Admin Portal—if this is left on, your Power BI reports will be released to the public.
- Disabling the 'Publish to web' setting as well—if this is left on, Power BI will publish your reports to the internet. Consider disabling publishing for the whole organization.
- Disabling the 'Share content with Monitoring the exported data iif printed or used in softcopy by youremployees- Consider turning off the 'export data' feature unless it's critically necessary.

Power BI apps and app workspace

Power BI enables shared development and staged deployment. You can publish content from your Power BI desktop into Azure workspaces. You can then add groups to the workspaces and assign users their roles and privileges as either viewer, contributor, member or admin.

The best practice here would be to implement a least-privilege administrative model. Workspace users should only log in with their given user account that has bare minimum permissions necessary for them to complete a task, nothing more.

When it comes to the publication of content, workspaces enable the neat packaging of content into single entities called apps. You can then delineate access privileges to these apps. A Recipient only views the report, Report Consumers are able to interact with but not edit the data,
while the App Author can make edits or updates as they like.

Row Level Security

Row-level security (RLS) can be implemented in Power BI desktop. It grants the ability to publish a single report to your user base but exposes the data differently to each person. RLS helps to secure data and streamline administration. Consider implementing RLS either in Analysis Services or in the Power BI data model.

The steps in the process include:

- Defining Power BI roles and rules and apply a DAX expression
- Validating roles and defining what users can see
- Managing security of the data model

Sharing Within your Organization, Guest Users and Sharing 'Outside the Walls

For stronger data protection, consider limiting Guest User creation on Power BI Tenant settings, Azure Active Directory settings, and Office 365 Security settings.

Power BI also enables the sharing of content by email, including personal email addresses. If you enable users to share content this way, by default, you will be enabling them to create guest accounts in Azure Directory. These guest users could then add content to workspaces or serve as admins.

Auditing

Admins and other users with the necessary privileges can access the Office 365 Admin Center. Here you can view exhaustive logs of all Power BI activities. Viewing these logs helps to monitor and evaluate access, users, and group activities,
including the sharing/exportation of reports on Power BI.

It would be wise to regularly access your audit logs so you can see who is doing what. That's acritical step in helping your organization comply with regulatory requirements on record preservation.

For more information, please contact us at:
Ivy Karlinsky | Ph: 425 869 8104 | E-mail: info@ilink-systems.com

Microsoft GOLD CERTIFIED Partner