Microsoft Purview Information Protection with NTT DATA

Projects that utilise Microsoft Office 365 and migrate multiple services to Azure Cloud are now part of the daily workload of many IT departments. The protection of confidential data also occupies one of the top places on the priority list for CISOs. Azure itself already provides an effective solution for protecting sensitive unstructured data: Purview Information Protection (PIP) with Azure Rights Management (ARM).

Word, Excel and many other types of documents travel in the age of cloud computing through a variety of technical infrastructures which are not controlled by their own company. The only really reliable way to protect sensitive data in such documents is therefore to couple security to the individual file itself. PIP provides a reliable answer to exactly this challenge: Intelligent classification makes it easy to see which business context the document is in and what level of confidentiality it has, regardless of the location. The question of whether and how the document should be protected can therefore be decided on the basis of the individual file and its content. Through file-based encryption (Azure Rights Management), the protection is also anchored into file itself so the user is able to travel with the encrypted file.

Data Centric Security

NTT DATA Security's Purview Information Protection service provides many benefits, which can include:

- Ensure document labelling is assigned correctly to sensitive and unsensitive data to reduce the risk of data leakage.
- Provide automatic document classification accurately which will provide added security to your organisation whilst saving employee time.
- Understand data flows within the organisation to suggest best practice with regards to how data should be classified and what labels should be used.

By utilising PIP, an organisation can classify personally-identifiable information (PII) that GDPR seeks to protect and enables technical controls implemented within PIP to limit data loss risks. As PIP can classify and protection data, it can support accidental data leakage or malicious leakage, therefore helping to reduce the risk of a GDPR breach from occuring.

Work Packages to Activate PIP/ARM

- Work packages to activate PIP / ARM
- Three-day workshop to assess the current status (licenses, affected areas of IT, affected areas of business) and development of an activation plan (high level)
- Creating a Data Map Using the PIP Scanner
- Analyse three particularly critical selected data flows
- Perform a PoC (policy design and installation of three test clients)
- Provide a step-by-step approach to enabling PIP / ARM across the enterprise
- Policy design and enterprise-wide rollout of PIP / ARM

The Challenge:

- Firewalls and infrastructure-based protection are inadequate in the age of the cloud.
- The protection of confidential documents must be ensured when using Office 365 / Azure.
- The introduction of data classify-cation in the enterprise seems complex and time-consuming.

Solution and Goal:

- Purview Information Protection with Azure Rights Management provides an effective technology that is already integrated with Office 365 / Azure.
- The protection and access rights are bound to the file itself.
- Smart Classification (Labelling) allows the contents of a file to decide on their protection - not their place of storage.

First Steps:

- Three-day workshop to develop an activation plan focusing on
  a) Licenses (often already in place)
  b) IT implications and
  c) Business impact
- Collecting inventory data with the PIP Scanner