NAVIGATING THE CHALLENGES OF SENSITIVE DATA PROTECTION: INSIGHTS FROM MICROSOFT

Safeguarding sensitive data is of high importance for businesses. The consequences of data breaches, including data loss, damage to stock prices, and hefty fines stemming from regulations such as the General Data Protection Regulation (GDPR), can be financially crippling. Moreover, these breaches erode the trust of individuals who fall victim to credit card fraud, identity theft, and other malicious activities resulting from such incidents. Alarmingly, the number of data breaches surged by 68 percent in 2021, reaching a 17-year high and incurring millions of dollars in losses. For instance, a single healthcare data breach impacted over 45 million people, tripling the figures from three years prior.

Sensitive data encompasses confidential information obtained by businesses from clients, job candidates, business partners, and employees. Examples of sensitive data categories include credit card numbers, Social Security Numbers (SSNs), personally identifiable information (PII) like home addresses and dates of birth, protected health information (PHI), and medical records that could be used to identify individuals.

To effectively tackle the challenges of sensitive data protection, Microsoft delves into four key threats and offers potential solutions:

1. Identifying the Location of Sensitive Data: Sensitive data within an organization can be concealed in unexpected corners. Implementing a robust data discovery process is imperative to ensure the proper safeguarding of sensitive information, as data scans can uncover these concealed storage locations.

2. Sorting Data by Importance: For an accurate risk assessment, data categorization must factor in the sensitivity and business impact of the data. Microsoft employs several categories, including non-business, business, general, confidential, and highly confidential, to aid in this process. Implementing security tools that automate the tagging of sensitive data across the organization can alleviate the challenges of manual data designation.

3. Safeguarding Critical Data: Chief Data Officers (CDOs) and Chief Information Security Officers (CISOs) bear the responsibility of protecting data while ensuring it flows through procedures and processes that maintain security without hindering workplace productivity.

4. Controlling Data to Mitigate Unnecessary Risks: Effective data control ensures that data remains discoverable, accurate, trustworthy, and secure. Proper data retention is crucial, as excessive storage can increase the volume of data exposed in a breach, while premature data disposal can pose legal risks.

To address these concerns, Microsoft suggests the following strategies for handling sensitive data:

- **Comprehensive Data Discovery:** Conduct thorough data discovery to identify all locations where sensitive data resides, aided by support for sensitive data types that can identify data using predefined or customized patterns.

- **Automation-Driven Data Classification:** Employ technology-driven data classification processes instead of relying solely on manual efforts.

- **Integrate Data Protection into Business Procedures:** Incorporate data protection seamlessly into existing business processes. Microsoft offers audit features that allow for data monitoring without disrupting operations, alongside data leakage prevention tools to safeguard critical data.

- **Invest in Data Protection Techniques:** Given the high cost of security breaches, invest in data discovery, data categorization, and data protection procedures.

Microsoft provides a range of products for information protection and governance:

1. **Microsoft Purview Information Protection:** This tool helps organizations discover, classify, and protect sensitive information, regardless of its location.

2. **Microsoft Purview Data Lifecycle Management:** Utilize Purview Data Lifecycle Management capabilities to govern data for compliance and regulatory requirements.

3. **Microsoft Purview Data Loss Prevention:** Apply consistent policies across cloud, on-premises environments, and endpoints to monitor, prevent, and remediate risky activities involving sensitive data.

In conclusion, safeguarding sensitive data is an essential aspect of modern business operations, and Microsoft offers a suite of tools and strategies to address the challenges associated with its protection and governance. Effective implementation of these measures can help organizations mitigate risks, maintain compliance, and protect their reputation and financial well-

being. IBSCY, as Microsoft Gold partner in Cyprus, is your go-to expert for professional IT services and solutions. We cater to businesses of all sizes, offering comprehensive expertise to safeguard your sensitive data effectively.

Learn more in Microsoft