CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

DATA PROTECTION MANAGEMENT – How is Data Protected?

OVERVIEW OF DATA PROTECTION MANAGEMENT

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management (DPM).

The DPM capability is intended to provide additional protections to the most critical mission data and systems on federal civilian networks. While the other CDM capabilities provide broader protections across federal networks, the DPM capability is focused on protecting sensitive (especially private) data within the agency. Protecting sensitive data requires security and privacy protections at rest, in use, and in transit to ensure the integrity, availability, and confidentiality of data and data assets. The CDM Program employs the DPM capability to help agencies and industry partners strengthen data protections to include identifying sensitive data, classifying data assets based on severity and impact, supporting timely response procedures to notify stakeholders of data breaches or spillage, and more. DPM helps agencies protect sensitive data through five capabilities: data discovery/classification (DATA_DISCOV), data protection (DATA_PROT), data loss prevention (DATA_DLP), data breach/spillage mitigation (DATA_SPIL), and information rights management (DATA _IRM).

BENEFITS OF DATA PROTECTION MANAGEMENT

The DPM capability focuses on providing agencies with the tools necessary to protect sensitive and private data in their networks. These tools allow agencies to ensure sensitive data is properly secured and stored by: (1) identifying sensitive data assets; (2) classifying the severity and impact of such assets; (3) identifying authorized roles, users, and policies for retention of private data; (4) collecting and reporting on data asset compromise; (5) developing timely response procedures to notify stakeholders of data breaches or data spillage and how to effectively recover from an attack; and (6) implementing standard cryptographic controls and mechanisms, such as FIPS-140-2 or data obfuscation.

DATA PROTECTION MANAGEMENT CAPABILITIES

The CDM Program leverages commercial-off-the-shelf tools to provide the following five DPM capability offerings:

Data discovery/classification

DATA_DISCOV provides techniques for identifying, discovering, and classifying data. This capability consists of the collection and reporting of information that provides consistent identification of data assets across the agency environment for processing, storing, and transmitting data. This CDM capability includes functions such as automated data discovery, which allows tools to scan targeted databases to identify sensitive data (e.g., usernames and addresses). Identifying and discovering data will help agencies obtain a better understanding of where sensitive data is on their network in order to protect it.

Data protection

DATA_PROT shows agencies two methods for protecting sensitive data. The first method is the application of cryptographic[1] technology. Encryption protects confidentiality by translating sensitive data into another form that can only be accessed with the proper decryption key. Encryption can be used to protect data at rest (e.g., stored in a database or on a hard drive) and data in transit (e.g., sent over the Internet). The second method protects sensitive data using data masking or obfuscation methods. Data masking/obfuscation involves applications that are programmed to replace data fields that contain sensitive data with substitute data that is generated based on a set of rules. Through these methods, agencies can better protect themselves from malicious interception or exfiltration of data stemming from internal or external sources.

Data loss prevention

DATA_DLP describes techniques to minimize the loss of data by providing consistent protection to block unauthorized exfiltration of sensitive data. The functions associated with this capability include exfiltration alerts and prevention, role-based data protection, and enhanced protections for sensitive information, such as Personally Identifiable Information. DATA_DLP allows an agency to limit, or prevent entirely, data exfiltration from data assets or other key infrastructure components.

Data breach/spillage mitigation

DATA_SPIL provides techniques for response and recovery activities resulting from a data breach or spillage. This capability assists agencies in developing strategic procedures to analyze, protect, and recover from data breaches. It uses specialized tools to identify specific points of failure that caused the data breach, quantify sensitive data lost or exfiltrated from a data spillage, calculate a mean time to recovery of standard operations, and develop new or enhance existing data security and privacy controls to prevent future data breaches. Through DATA_SPIL, agencies can understand how a data breach happened, develop the necessary steps to resume normal operations, and prevent against future attacks or breaches.

Information rights management

DATA_IRM provides controls for access relating to enterprise information (e.g., documents, files). This capability utilizes tools that employ cryptographic controls for encrypting sensitive data, a granular control system for least-privilege access, and identification mechanisms for authenticating users.

CURRENT STATE OF CDM DATA PROTECTION MANAGEMENT DEPLOYMENT

The CDM Program has a DPM pilot underway on three high-value assets at one agency, with a goal of broadening to multiple agencies. The CDM Program continues to reach out to agencies to obtain interest in conducting DPM pilots. Lessons learned from these pilot efforts will inform the CDM DPM approach as it expands to full-scale support for in the coming years.

For more information on DPM capabilities and/or the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.

[1] Cryptographic security includes both encryption and hashing.