

Datenschutz durch Technikgestaltung

RDX-Wechselplattentechnik erfüllt DSGVO-Anforderungen



Auch wenn die DSGVO nicht die Hauptaufgabe für IT-Verantwortliche ist, sorgt sie insbesondere bei kleinen und mittleren Firmen für Kopfzerbrechen. Datenschutz und Datensicherung sind ohnehin ein Muss, auch vor dem Hintergrund anderer regulatorischer Vorschriften, den Datenschutzeempfehlungen des BSI oder etwa Cyberattacken. Um dem besser begegnen zu können, sind beispielsweise Wechselplattensysteme wie RDX geeignet.

Die DSGVO mit ihren 99 Artikeln in elf Kapiteln soll dem Schutz der Privatsphäre und der Verarbeitung personenbezogener Daten dienen. Die gute Nachricht: Viele Bereiche des Datenschutzes werden durch die DSGVO gar nicht neu geregelt, sie erhalten jedoch neue Brisanz durch drohende Strafen bzw. die Furcht vor Abmahnwellen. Immerhin führt die Verordnung dazu, dass auch kleine und mittlere Unternehmen (KMUs) ihre Datenhaltung auf den Prüfstand stellen: Was wird wo gespeichert, gesichert und archiviert? Wie lange werden die Daten vorgehalten? Laut Art. 25 Absatz 1 der DSGVO sind Unternehmen und Organisationen angehalten, »geeignete technische und organisatorische Maßnahmen« (TOM) in die Wege zu leiten, die darauf ausgelegt sind, die Privatsphäre zu schützen und Datenschutzgrundsätze zu garantieren. Außerdem geht es hier um »Datenschutz durch Technikgestaltung«, und diese obliegt am Ende als Teilaspekt der DSGVO doch der IT-Abteilung.

Datenvorhaltung und Technologiewahl

Im Grundsatz gilt es dabei Wege zu finden, um Daten zu sichern, vorzuhalten und gegebenenfalls zu löschen. Daten müssen zugänglich gemacht werden können, unabhängig davon, ob sie Online-Speicher, Backup oder Archiv sind. Da dies in der Regel über zehn Jahre oder länger gewährleistet werden muss, ist die Wahl einer geeigneten Speichertechnik gut zu überdenken. Letztlich bleibt jedoch eine Datensicherungsstrategie mit Wechselmedien notwendig, die Auslagerung von Daten auf sicheren, widerstandsfähigen Medien ein Muss. Dazu eignen sich die robusten RDX-Medien von Overland-Tandberg. Sie kombinieren die Portabilität und Zuverlässigkeit des Bandes mit der Geschwindigkeit einer Festplatte. Auf Dateien kann schnell und direkt im File-System zugegriffen werden, die Systeme sind leicht zu bedienen und kompatibel mit gängiger Backup-Software inklusive Bordmitteln wie Windows Backup oder Apple Time Machine. RDX-Medien sind dafür äußerst robust gebaut, für eine Lebensdauer von mehr als zehn Jahren konzipiert, vollständig rückwärts- und vorwärtskompatibel und somit immer in einem RDX-Laufwerk ohne technologiebedingten Migrationsaufwand nutzbar, bieten einen Datendurchsatz von bis zu 1,2 TByte/h und Speicherkapazitäten von bis zu fünf TByte pro Wechselmedium und medienübergreifende Sicherungsmöglichkeiten.

Zugangskontrolle und Verschlüsselung

Laut DSGVO müssen die personenbezogenen Daten vor einer »unbefugten Offenlegung« und unbefugtem Zugriff geschützt sein. Dies betrifft letztlich die Möglichkeit, Datenträger einer Policy-basierten Zugangskontrolle zu unterziehen. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Ein weiterer aufgeführter Punkt besteht in der Notwendigkeit der »Pseudonymisierung und Verschlüsselung« personenbezogener Daten und der »Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen«. Dies ist insbesondere für den Datentransport und -austausch ein entscheidendes Kriterium. Die RDX-Technologie adressiert diese technischen Teilaspekte durch eine Reihe von neueren Entwicklungen. Zunächst basieren RDX-Systeme auf herkömmlicher Festplattentechnik, die den meisten Anwendern insbesondere bei KMU vertrauter sein dürfte als das Magnetband oder Cloud-Lösungen.

Die Medien sind uneingeschränkt kompatibel über alle Produktgenerationen hinweg, was bei der Wiederherstellung archivierter Daten ein enormer Vorteil ist. Mit der RDX Cartridge Encryptor-Software (RCE) steht zudem eine freie Software-Anwendung zur Verfügung und erlaubt unkomplizierte Verschlüsselung aller auf RDX gesicherten Daten. Die Software ist für einfache und effiziente Nutzung konzipiert, basiert auf dem AES-256-Encryption-Industriestandard, welcher zugleich Secure Erase-nach NISP-Standard zur lückenlosen Beseitigung von Daten und Programmen als auch die Funktionalität zum Löschen von Schlüsseln (Cryptographic Key Deletion). Die RDX-Verschlüsselungs-Software bietet damit KMUs eine kostenfreie Lösung für die sichere Speicherung ihrer Daten.

Hardware-Verschlüsselung entspricht höchsten Standards

Mit RDX PowerEncrypt steht für die Wechselplattentechnologie auch eine Hardware-basierte Verschlüsselung auf 56-AESXTSSstandard zur Verfügung. Die Hardware-basierte Verschlüsselungstechnik ist im Vergleich zu Software einfacher zu handhaben, belastet die Prozessorleistung nicht und erzeugt keine Konflikte mit Betriebssystem- und anderen Software-Ständen. Der schnellste heute verfügbare Super- Computer ist theoretisch in der Lage, pro Sekunde 10^{14} Schlüssel zu erzeugen und würde damit $3,31 \times 10^{56}$ Jahre benötigen, um herkömmliche 256-AES-Verschlüsselung zu entschlüsseln. Durch Parallelisierung und zukünftig über Cloud-Services angebotene größere Rechenleistung wird es möglich sein, die herkömmliche 256-AES-Verschlüsselung zu knacken. Mit RDX PowerEncrypt wird die Schlüsseleingabe auf einen Schlüssel pro Sekunde begrenzt und ist so robust, dass die Software sogar Hacker-Parallel-Cracking-Techniken widerstehen kann, die verwendet werden, um die Crackzeit zu reduzieren. Die RDX-PowerEncrypt-Verwaltung über den RDX-Manager unterstützt dabei bis zu acht Nutzer mit unterschiedlichen Rechteprofilen und Zugangshierarchien, eine optionale, automatische Laufwerksidentifikation sowie die Analyse der Passwortsicherheit bei der Einrichtung.

Von FIPS bis KPMG – Zertifizierte Lösungen bringen Sicherheit

RDX PowerEncrypt in der ersten Produktversion unterstützt derzeit interne RDX-SATA-III-Laufwerke und-Medien unter Windows. In dieser Konfiguration wird es in 2018 auch FIPS 140-2 validiert werden. Der FIPS 140-2 (Federal Information Processing Standard) ist ein Standard der US-Regierung und beschreibt die Verschlüsselung und die zugehörigen Sicherheitsanforderungen, die IT-Produkte zur vertraulichen Nutzung erfüllen sollen. Der Standard gewährleistet, dass ein Produkt solide Sicherheitspraktiken wie etwa zugelassene, starke Verschlüsselungsalgorithmen und -verfahren einsetzt. Zudem legt er fest, wie Einzelpersonen oder Prozessabläufe zur Nutzung des Produkts autorisiert werden müssen und wie Module oder Komponenten zur sicheren Interaktion mit anderen Systemen entwickelt werden müssen. Die Validierungsstufe FIPS 140-2 gilt als Zeichen für Sicherheit und Qualität und zertifiziert allen Käufern, dass die Voraussetzungen für Sicherheitsprodukte erfüllt sind.

WORM-Technologie (Write Once Read Many) eignet sich für die Archivierung gemäß regulatorischer Anforderungen. Die rdxLOCK-Software wurde jüngst durch die Wirtschaftsprüfungsgesellschaft KPMG zertifiziert und damit die integrierte WORM-Funktion für eine Vielzahl an nationalen und internationalen Anforderungsstandards im Buchhaltungs-, Rechnungs- und Steuerwesen frei gegeben.

Diese WORM-Funktion ist damit geeignet, um alle Anforderungen aktueller und zukünftiger Compliance-Regeln wie der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) zu erfüllen.

In der Debatte um die Umsetzung der DSGVO bleiben »geeignete technische und organisatorische Maßnahmen« (Art. 25 Absatz 1) gefordert, die in Hard- und Software und geeigneten Prozessen umgesetzt werden müssen. Die RDX-Technologie mit Wechseldatenträgern, Einzellaufwerken oder Appliances und der entsprechenden Software kann dabei neben anderen Speichertechnologien wertvolle Hilfe leisten: Datenschutz durch Technikgestaltung!