Abstract/Steckbrief

für Vortrag beim GI-Fachgruppentreffen am 18.+19. Oktober 2018 in Coburg

Autor: Alexander Wollheim

Hochschule Coburg, Alexander.Wollheim@stud.hs-coburg.de

Thema:

Data Encryption im Mainframebereich (z/OS) – am Beispiel von Data Set Encryption und Encryption im Db2

Motivation:

Die HUK-COBURG ist ein Versicherungsunternehmen, welches viele Daten von Kunden in Datenbanken auf Großrechnern speichert. Diese Daten umfassen vor allem persönliche Daten (Name, Anschrift, Alter usw.) und Vertragsdaten.

Da die HUK-COBURG diese Kundendaten speichert und verwaltet, unterliegt sie den aktuellen Datenschutzgesetzen und ist dazu verpflichtet, diese jederzeit einzuhalten. Da immer neue Gesetze hinzukommen, kann es notwendig werden, die Daten direkt in den Datenbanken auf dem Großrechner zu verschlüsseln.

Im Versicherungsunternehmen wird die aktuellste Großrechnergeneration, die z14, von IBM betrieben. Dieser Großrechner läuft mit dem Großrechnerbetriebssystem z/OS. Als Datenbanksystem wird das ebenfalls von IBM vertriebene Db2 eingesetzt. Neben der Speicherung von Kundendaten in Db2-Datenbanken, werden zur Datenverwaltung unter z/OS sogenannte Data Sets verwendet. Data Sets können in verschiedenen Arten vorkommen. Dazu zählt z. B. das Partioned Data Set, welches vergleichbar mit einem Ordner, der mehrere Dateien besitzt, ist und das Sequential Data Set, welches mit einer Textdatei gleichgesetzt werden kann.

Wird im Großrechnerumfeld auf z/OS-Basis von Verschlüsselung von Daten gesprochen, verwendet man häufig den Begriff Data Encryption. Diese Arbeit beschäftigt sich mit der Data Encryption direkt im z/OS auf Data Set Ebene und der Data Encryption im Db2. Derartige Arten der Verschlüsselung werden bisher noch nicht von der HUK-COBURG eingesetzt.

Mit dem Upgrade auf die aktuellste Großrechnergeneration ergibt sich eine neue kostengünstige Möglichkeit zur Verschlüsslung der Daten.

Mit der Einführung der IBM z14 wurden neue Hardwarekarten für Verschlüsselungsprozesse und Data Encryption verbaut. Diese Karten werden als Kryptokarten bezeichnet, sind aber noch nicht freigeschaltet und konfiguriert, da sie aktuell nicht verwendet werden. Durch den Einsatz der Kryptokarten kann die Verschlüsselung, welche bisher nur rein durch Software möglich wäre, auf die Kryptokarte ausgelagert werden. Eine rein durch Software durchgeführte Verschlüsselung würde enorme Kosten verursachen, da im Mainframebereich die CPU-Nutzung bezahlt wird. Diese CPU-Nutzung wird durch den Einsatz der Kryptokarten bis auf einen kleinen Teil der Instruktionen auf die Karte ausgelagert. Laut IBM soll der Einsatz der Kryptokarten die Performance bei der Verschlüsselung dramatisch erhöhen und die Kosten merklich verringern.

Bisher wurden noch keine Untersuchungen in Bezug auf diese neue Verschlüsselungsmöglichkeit von der HUK-COBURG durchgeführt, da es noch kein Gesetz

gibt, welches die Verschlüsselung auf einer solchen Ebene vorschreibt. Sowohl Machbarkeit, Performance (z. B. Antwortzeiten) und Kosten beim Einsatz der Verschlüsselung sind Faktoren, die für eine spätere Anwendung von Data Encryption entscheidend sind.

Problemstellung und Ziel:

Die HUK-COBURG hat bisher noch keine Erfahrungen im Bereich der Verschlüsselung von Data Sets und Daten im Db2 auf der Plattform z/OS.

Die mit der z14-Hardware neu hinzugekommenen Kryptokarten und die neuen Verschlüsselungsmöglichkeiten, die Db2 bietet, sollen deshalb im Rahmen einer Bachelorarbeit untersucht werden. Das Ziel dieser Untersuchung ist es, eine Machbarkeitsuntersuchung zum Einsatz von Data Encryption durchzuführen, die für spätere Entscheidungen bei der Weiterentwicklung des Unternehmens herangezogen werden können.

Für diese Untersuchungen sind verschiedene Fragen bzw. Probleme zu klären. Diese unterteilen sich in grundlegende, technische und konzeptionelle Fragen bzw. Probleme. Diese Fragen und Probleme werden im Vortrag näher erläutert.