Goetz & Patak
Rechtsanwälte

Sascha Daniel Patak
Dr.iur. Rechtsanwalt
Oberwachtstrasse 13
8700 Küsnacht ZH
Direkt +41 44 991 1211
Office +41 44 991 1212
Fax +41 44 991 12 65
sp@gplegal.ch /www.gplegal.ch

Gutachten

Sicherheit MOUNT10 COMBO ECO PRO aus rechtlicher Sicht

Fragestellung

Entspricht die Sicherheit und Funktionalität des Backups mit MOUNT10 dem heutigen IT-Security-Standard sowie den rechtlichen Anforderungen an ein Backup nach Schweizerischem Recht?

Zusammenfassung

Die Backup Versionen COMBO, ECO und PRO der MOUNT10 AG erfüllen die rechtlichen Voraussetzungen für ein Backup. In Bezug auf die Lagerung (SWISS FORT KNOX) sowie die Überwachung (digitale Kontrolle jedes Accounts kombiniert mit manuellem Interventionsprozess) werden die Mindestanforderungen sogar weit übertroffen[i].

Ausgangslage

MOUNT10 AG, eine Aktiengesellschaft mit Sitz in Baar, Kanton Zug, bietet ein Backup-System an, welches vom Kunden ausgewählte Dokumente über das Internet auf ein Backup-System (dedizierte Hardware oder gemeinsam genutzter Speicher) sichert. Dabei werden drei verschiedene Versionen unterschieden. Es sind dies MOUNT10 COMBO, ECO und PRO. Standort der Backup-Systeme ist das so genannte „SWISS FORT KNOX“, eine

Hochsicherheitsanlage in ehemaligen sowie aktiven Festungsanlagen der Schweizer Armee.

Rechtliche Grundlagen

Aus rechtlicher Sicht ergeben sich verschiedene Grundlagen, welche einen direkten Einfluss auf die technischen Gegebenheiten der Datensicherung und der Datensicherheit haben. Ein eigentliches Gesetz zur Datensicherung (Backup) besteht nicht. Dafür ergeben sich aus den Gesetzen diverse Anforderungen direkt oder indirekt. In zivilrechtlicher Hinsicht ergehen Anforderungen aus Aufbewahrungspflichten (vor allem Art. 962, Abs. 1 OR[ii], Art. 6 ff. GeBüV[iii]) sowie Sicherungspflichten bezüglich Persönlichkeitsschutz und Geheimhaltung (Art. 28 ZGB[iv] generell, Art. 328b OR für Arbeitnehmer, vertragsrechtliche Geheimhaltungs- und Sorgfaltspflichten). Im Weiteren gelten grundsätzlich für die Durchsetzung jedes zivilrechtlichen Anspruches Art. 8 ZGB, wonach derjenige das Vorhandensein einer behaupteten Tatsache zu beweisen hat, der aus ihr Rechte ableitet. Fehlende Beweisbarkeit bedeutet Rechtsverlust.

In öffentlich rechtlichem Bereich gelten insbesondere Aufbewahrungspflichten im Bereich der Mehrwertsteuer- und Steuergesetzgebung sowie Datenschutzbestimmungen (insbesondere DSG). Hinzukommen für bestimmte Tätigkeiten Geheimhaltungs- und Sorgfaltspflichten (für Anwälte und Ärzte Art. 321 StGB, Sorgfaltspflichten für Geschäftsführung, Buchführung etc.).

Sowohl in zivil- wie auch öffentlich rechtlichen Bereichen wird grundsätzlich nicht über den Standard der Sicherheit gesprochen. Es ist aber aufgrund der ISO-Zertifikate sowie der diversen Standards, eingesetzt in E-Banking, digitalen Versendungsdiensten, eidgenössischen Anwendungen davon auszugehen, dass ein mindestens einfaches Backup für mindestens 4 Wochen gesichert und digital geschützt vor ungerechtfertigtem Zugriff (DSG) bestehen muss. Dieses muss – sofern ferngewartet – ebenfalls gesichert übermittelt werden.

Backup durch MOUNT10

Hardware

Die Daten werden auf Harddisks in beiden Rechenzentren gespiegelt aufbewahrt. Die Harddisks werden softwaremässig und manuell gewartet und überprüft, zudem regelmässig ersetzt.

Speziell ist sicher der Aufbewahrungsort. Die Server stehen in aktiven sowie ehemaligen militärischen Festungsanlagen mit höchsten Sicherheitsvorkehrungen. Der physische Zutritt erfolgt äusserst restriktiv (mehrere tonnenschwere Panzertüren, verschiedene Sicherheitsbereiche und -Schleusen, vollumfängliche Kameraüberwachung, Vieraugenprinzip). Die Räume sind speziell gesichert und entsprechen den neusten Anforderungen. USV-Anlagen sowie Dieselgeneratoren gewährleisten die Stromversorgung im Notfall. Das Kühlsystem wird durch einen unterirdischen See gespiesen. Diese Lösung der Lokalität ist in dieser Form sicher einzigartig und entspricht einem unerreichten Sicherheitsniveau.

Software

Das Backup der MOUNT10 (alle Versionen) erfolgt inkrementell und entspricht grundsätzlich dem heute gängigen Modell einer Datensicherung.

Die Wahl der Daten wird über eine Software mit grafischer Benutzeroberfläche durch den Kunden selber vorgenommen. Dies hat den Vorteil, dass kundenspezifisch die schützenswerten Daten angewählt werden können. Es birgt aber das Risiko, wichtige Daten zu vergessen.

Die gewählten Daten werden in der Software auf dem Kunden-Infrastruktur aufbereitet. Sie werden dabei über eine 128 Bit SSL verschlüsselte Verbindung an den Server im SWISS FORT KNOX gesandt. Damit sind die Daten auf dem Weg gesichert, wenn auch unverschlüsselt.

Die Daten werden im SWISS FORT KNOX direkt auf dem RAM (also vor der effektiven Speicherung) verschlüsselt. Dabei werden Daten und der Encryption Key über die SSL-Verbindung mitgesandt und ausschliesslich im Cache gespeichert, also sofort wieder überschrieben. Gemäss Aussage des Software-Betreibers ist die Speicherung so programmiert, dass sie ausschliesslich auf dem RAM-Baustein erfolgen kann, womit sie nur auf einem flüchtigen und fortwährend überschriebenen Medium uneinsehbar für Dritte nur für sehr kurze Zeit existiert. Diese Speicherung der ankommenden Daten und des Encryption Keys auf einem flüchtigen Speicher im hochgeschützten Datacenter erfüllt damit die gesetzlichen Grundlagen, insbesondere auch diejenigen der Geheimnispflicht und des Datenschutzes, da Daten und Key zu jedem Zeitpunkt gesichert sind und nicht durch Dritte eingesehen bzw. verwendet werden können. Weiter bildet die direkte Verschlüsselung am Kundenstandort in der Version PRO eine nochmals höhere digitale Sicherheit, da die Daten den Betrieb niemals unverschlüsselt verlassen. Die gesetzlichen Voraussetzungen sind aber für alle Versionen erfüllt.

Zusammenfassend kann man damit festhalten, dass die technische Sicherheit i.S. Transport und Lagerung dem heutigen IT-Security-Standard hochsicherer Daten genügt.

Weitere Sicherungsmassnahmen

Das gesamte System, wie deren Abläufe, die Backup-Prozesse jedes einzelnen Kunden sowie die Übertragungsrate und Datenmenge werden digital gemessen und überwacht. Unregelmässigkeiten werden mittels Systemmeldung dem Kunden per Email mitgeteilt (z.B. bei fehlendem Backup).

Zusätzlich wird jeder einzelne Backup-Account (Einzelarbeitsplatz oder Server) täglich manuell mittels eigens dafür definierten Interventionsprozess durch einen Mitarbeiter auf Unregelmässigkeiten im Bereich Datenfluss, Datenmenge, Backup-Prozedere und weiteres hin kontrolliert. So werden

gemäss verifizierter Aussagen der betreuenden Personen – weitere, durch Software alleine kaum feststellbare Unregelmässigkeiten behoben[v]. Die Daten selber, bzw. deren Richtigkeit können nicht überprüft werden, da diese vollverschlüsselt sind und zu keinem Zeitpunkt unverschlüsselt durch die Mitarbeiter der MOUNT10 einsehbar sind.

Diese Kombination von computergesteuerten und manuellen täglichen Kontrollen ergibt eine sehr weitreichende Sicherheit, wie sie sonst nur durch firmeneigene Softwareabteilungen überhaupt erreicht werden können.

Es ist im Weiteren darauf hinzuweisen, dass die Daten selber aufgrund ihrer Verschlüsselung nur auf die technische Vollständigkeit und korrekte Verschlüsselung hin überprüft werden können. Dieses Problem stellt sich aber allen verschlüsselten Systemen gleichermassen. Es bleibt daher Aufgabe des Kunden, durch effektive Desaster-Recovery-Tests in regelmässigen Abständen das gesamte System zu überprüfen. Durch den Gutachter durchgeführte Tests haben zu keinen Problemen geführt.

Küsnacht, 23.11.2010

Dr.iur. Sascha D. Patak

---

[i] Diese Erkenntnis entspricht der detaillierten persönlichen Beurteilung des Gutachters und gibt seine Rechts- und Tatsachenauffassung wieder.

[ii] Obligationenrecht (SR 220; Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

[iii] Geschäftsbücherverordnung (SR 221.431; Verordnung über die Führung und Aufbewahrung der Geschäftsbücher

[iv] Schweizerisches Zivilgesetzbuch (SR 210)

[v] Als Beispiel wurde genannt: Korrekte Backups mit fälschlicherweise fehlender oder nur sehr kleinen Backup-Datenauswahl (0k z.B). Das Backup wird korrekt durchgeführt, der Kunde jedoch hat versehentlich die Datenauswahl verändert oder ganz gelöscht. Technisch ist das Backup richtig, materiell wurden aber keine Daten übertragen.