

Datenklau von Bankkundendaten – Strafbarkeit des Datendiebstahls und Präventionsmassnahmen

Roman Haltinner

Dipl. Wirtschaftsinformatiker
MAS Economic Crime Investigation
ISO27001 Lead Auditor
Certified Information System Auditor, CISA



Roman Haltinner verfügt über 20 Jahre Berufserfahrung in den Bereichen Informationssicherheit, Cyber Security, Datenschutz und IT Forensik. Er sammelte umfassende Beratungs- sowie operative Erfahrung in den folgenden insbesondere in den Bereichen von Cyber Security; diesen Themen und berät und unterstützt (multi)nationale Kunden in der Finanzdienstleistungsbranche, Industrie sowie Behörden in Projekten. Er war 11 Jahre lang beim Wirtschaftsprüfungsunternehmen KPMG für den Aufbau und die operative Führung des Fachbereich Cyber Security verantwortlich. Er war maßgeblich an der Entwicklung der globalen KPMG Methode für Cyber Security Assessments beteiligt und vertrat KPMG in diesem Thema bei der FINMA. Künftig wird er bei Ernst & Young den Bereich Cyber Risk (GSA) als Partner leiten.

Die Masterarbeit befasst sich mit der Fragestellung, wie Datendiebstahl von Bankkundendaten rechtlich einzuordnen ist und welche Präventivmassnahmen in regulatorischer, rechtlicher und organisatorischer Sicht eine Bank im Falle eines Datendiebstahls oder einer Preisgabe von Daten zu ergreifen hat.

Ausgangspunkt der Arbeit stellt die Vermittlung eines Begriffsverständnisses dar. Begriffe wie Information und Daten im Kontext der Rechtslegung sowie der Informatik, sollen abgeglichen und verstanden werden. Zudem werden Begrifflichkeiten im Zuge der rechtlichen Anforderungen wie Sicherheit und Datenschutz geklärt. Ausgehend von diesem Definitionsverständnis folgt eine Einführung in die konkreten Problemstellungen mittels Aufzeigen von Geschehnissen auf dem Bankenplatz Schweiz. Daraus stellen sich Schlüsselfragen zur Strafbarkeit von Datendiebstahl und Datenhehlerei sowie zur Verantwortung der Bank.

Der zweite Teil behandelt rechtliche und kriminalistische Aspekte des Datendiebstahls. In einem ersten Schritt werden Datendiebe, ihre Motive und Angriffsmethoden beleuchtet. Daraus ergibt sich die Beschreibung der Bedrohungen, aus welchen die Präventionsmassnahmen abgeleitet werden. Anhand von Praxisbeispielen von Datendiebstahl von Bankkunden, eines Innentäters sowie einer Tathandlung eines Cyberkriminellen von ausserhalb der Bank wird die Aktualität der Thematik verdeutlicht. Anschliessend wird Datendiebstahl aus materiell strafrechtlicher Hinsicht anhand von Straftatbeständen analysiert und die Fragestellung, ob auch Datenhehler und Nutzniesser zur Verantwortung gezogen werden können, eingehend erörtert. Da es sich bei der Problematik um Bankdatendiebstahl von globaler Bedeutung handelt, findet auch die Rechtslage im Ausland in einem überblicksartigen Kapitel Berücksichtigung. Insbesondere in den USA und der EU, namentlich in Deutschland.

Der dritte Teil der Arbeit richtet sich darauf, mit welchen präventiven Massnahmen Banken dieser besonderen Form der Wirtschaftskriminalität begegnen können. Das erste Kapitel

dieses Teils geht auf die neuen Regulationen der Schweizerischen Finanzmarktaufsicht (FINMA) und der Schweizerischen Bankiervereinigung (SBV) ein und beleuchtet die internationalen Richtlinien der Finanzmärkte Grossbritannien und Singapur. Die Bedrohungen und Risiken sowie die rechtlichen Anforderungen in Bezug auf Datendiebstahl werden unter Berücksichtigung der vorangegangenen Themenschwerpunkte analysiert und in einem Massnahmenkatalog zur Bekämpfung von Datendiebstahl beschrieben. Das Hauptaugenmerk wird auf die organisatorischen und personellen Massnahmen gelegt, da die technischen Massnahmen den Rahmen dieser Arbeit sprengen. Trotzdem werden einige technische Massnahmen, welche aus regulatorischer Sicht gefordert und im Zusammenhang mit Massnahmen im Umgang mit Datendiebstahl unerlässlich sind, überblicksartig behandelt.

Als Ergebnisse der Analyse wurde ein „Leitfaden Prävention Datendiebstahl“ für die Praxis erstellt, der eine Hilfestellung für Banken und Effektenhändler bieten soll. Abgerundet wird die Arbeit von einer abschliessenden Würdigung und einem Ausblick in die Zukunft dieser Thematik.

Dem Autor ist in der Schweiz kein vergleichbares Werk bekannt, welches eine ganzheitliche Erfassung der rechtlichen Anforderungen, Betrachtung kriminalistischen Aspekte und der präventiven Umsetzung in Form von organisatorischen und technischen Massnahmen in Bezug auf den Diebstahl von Bankkundendaten beschreibt. Die in dieser Arbeit referenzierten Anforderungen der Regulatoren und gängigen Standards, decken dieses Themenfeld nur teilweise ab. Die Massnahmen im Leitfaden sind gezielt auf die Bedrohung des Datendiebstahls von aussen und innen ausgerichtet und basierend auf dem Wissen und den Erkenntnissen des Modus Operandi solcher in der Arbeit beschriebenen Taten.

Die vorliegende Arbeit wurde im Herbstsemester 2013 verfasst und berücksichtigt Literatur, Rechtsprechung sowie allgemeine Entwicklungen und Unterlagen bis Ende November 2013.