Cyberfahnder-Newsletter 3 vom 07.03.2010

Vorratsdaten und Skimming

Der Cyberfahnder ist ein Freizeitprojekt. Die hat in den letzten Wochen der BGH mit mehreren Entscheidungen mit Bezug zum Skimming für sich in Anspruch genommen.

Arbeitspapier Skimming #2

Seit Ende Januar hat der BGH mehrere Entscheidungen mit Bezug zum Skimming veröffentlicht, die eine vollständige Überarbeitung des **Arbeitspapiers Skimming** (Link) erforderlich gemacht hat. Es umfasst jetzt 42 Seiten und der Teil über die Strafbarkeit der verschiedenen Erscheinungsformen des Skimmings wurde völlig überarbeitet. Hinzu gekommen ist eine Rechtsprechungsübersicht.

Der BGH hat jetzt im Zusammenhang mit dem Erwerb von Rohlingen für Zahlungskarten den Beginn des Versuches der Fälschung mit dem unmittelbaren Ansetzen zum Fälschen gleichgesetzt. Das lässt keinen Raum für vorgelagerte Handlungen, die in die Vollendung eines Tatbestandsmerkmals unmittelbar münden. Beim „klassischen Skimming“ ist das Ausspähen der Kartendaten eine notwendige Voraussetzung für die Fälschung. Das kann dazu führen, das Ausspähen als Einstieg in den Versuch anzusehen.

Der 2. Senat des BGH betrachtet das Ausspähen der Daten auf den Magnetstreifen von Zahlungskarten nicht als ein Ausspähen von Daten im Sinne von § 202a Abs. 1 StGB, weil den Karten Sicherheitsvorkehrungen gegen das Ausspähen fehlen.

Diese Argumentation ist schlüssig und nachvollziehbar. Der einzige Haken ist dabei, dass das BVerfG im Zusammenhang mit dem Urteil zur Onlinedurchsuchung einen besonderen Rechtsschutz zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verlangt. Eine verfassungskonforme Auslegung hätte erwarten lassen, dass dieser Schutz auch im Rahmen des § 202a StGB zum Tragen kommt, weil ein Schutzmechanismus immerhin die bewusste Entscheidung des Karteninhabers ist, auf die Integrität des Geldautomaten zu vertrauen und die Zahlungskarte in den Kartenleseschacht einzustecken.

Die Strafbarkeit im Vorbereitungsstadium habe ich neu betrachtet und komme zu differenzierten Ergebnissen.

Der „Umgang“ mit Kartenlesegeräten (Skimmern) dürfte von § 149 StGB umfasst und mit Freiheitsstrafe bis zu 5 Jahren bedroht sein.

Die Programme in PIN-Skimmern – Tastaturaufsätze und Kameras - sind aus § 263a Abs. 3 StGB mit 3 Jahren Freiheitsstrafe bedroht, wenn sie aus Bauteilen zusammengesetzt werden und über eine eigene Steuerung für das Speichern verfügen. Werden jedoch Mobiltelefone mit Kamerafunktion oder digitale Kameras verbaut, so wird zum Ausspähen das geräteeigene Programm verwendet. Ihm kommt das Dual use-Privileg zugute, das das BVerfG anerkennt. Weil § 263a StGB nur Programme und nicht auch „ähnliche Vorrichtungen“ (§ 149 StGB) mit Strafe bedroht, scheidet eine Strafbarkeit wegen Umgangs aus.

Erst wenn Dual use-Programme zum Ausspähen von PIN erfolgreich eingesetzt werden, greift die Vorbereitungshandlung aus § 303b Abs. 5 in Verbindung mit § 202c StGB. Danach werden auch Zugangscodes geschützt und zwar spätestens dann, wenn 2 PIN nachweislich ausgespäht wurden. In diesem Fall werden die Täter mit Freiheitsstrafe bis zu einem Jahr bedroht. Hui.

Weitere Einzelheiten finden Sie im **Arbeitspapier Skimming.**

Der Umgang mit Verkehrsdaten nach dem Urteil des BVerfG

Am 02.03.2010 hat das BVerfG die §§ 113a und 113b TKG insgesamt für nichtig erklärt und § 100g StPO, soweit er den strafprozessualen Zugriff auf Vorratsdaten zulässt.

Ich bin kein Fachmann für Staats- und Verfassungsrecht. Dennoch treibt mich die Unruhe und

möchte ich wissen, wie ich mit den Vorratsdaten umgehen soll, die ich nach Maßgabe der diversen einstweiligen Anordnungen des BVerfG seit dem 11.03.2008 zulässigerweise erhalten habe. Seither durften die Zugangsprovider nur die Vorratsdaten herausgeben, die für die Ermittlungen im Zusammenhang mit Straftaten aus dem Straftatenkatalog des § 100a Abs. 2 StPO erforderlich sind.

Mein größtes Problem dabei ist, wie ich mit der Nichtigkeitserklärung als solche umgehen muss. Sie spricht für eine Unwirksamkeit von Anfang an (ex tunc). Das stimmt auch.

Von besonderer Wichtigkeit ist § 79 BVerfGG. Danach bleiben von der Nichtigkeitserklärung bestandskräftige Entscheidungen unberührt. Als Ausnahme ist vorgesehen, dass wegen nichtiger materieller Strafnormen die Wiederaufnahme des Verfahrens nach den Vorschriften der StPO ermöglicht wird.

§ 100g StPO ist eine Verfahrensvorschrift und nur im Hinblick auf den Zugriff auf Vorratsdaten als nichtig erklärt worden. Dank der vorläufigen Verfahrensregeln des BVerfG zur Anwendungspraxis und der Rechtsprechung zur unechten Rückwirkung dürfen die rechtmäßig erhobenen Vorratsdaten weiter verwertet werden und unterliegen keinem Verwertungsverbot (das hat mich ein weiteres Wochenende gekostet).

Das bedeutet im einzelnen:

► Seit dem 02.03.2010 darf gemäß § 100g StPO im Strafverfahren auf keine Vorratsdaten zugegriffen werden. Sie dürfen von den Zugangsprovidern nicht mehr gespeichert werden.

► Andere zurückliegende Verkehrsdaten, die die Zugangsprovider aus kaufmännischen oder technischen Gründen speichern dürfen, dürfen nach wie vor aufgrund eines Beschlusses nach § 100g StPO angefordert werden. Das dürfte einen Zeitraum von 3 Monaten in der Vergangenheit nicht überschreiten.

► Künftige Verkehrsdaten müssen die Zugangsprovider aufgrund eines Beschlusses nach § 100g StPO speichern und herausgeben.

► Die seit dem 11.03.2008 nach Maßgabe der einstweiligen Anordnung des BVerfG eingeführten Vorratsdaten unterliegen keinem Verwertungsverbot, wenn sie wegen Straftaten aus dem Straftatenkatalog des § 100a Abs. 2 StPO ermittelt wurden und die zugrunde liegende Straftat auch im Einzelfall besonders schwer wiegt.

► Das gilt auch dann, wenn sich der rechtliche Gesichtspunkt in der Zwischenzeit geändert hat, die prozessuale Tat aber dieselbe ist.

► Ausschlaggebend für die Zulässigkeit der Verwertung ist der Zeitpunkt der Einführung in das Verfahren. Er kennzeichnet den Grundrechtseingriff und erfordert die Prüfung anhand des (seinerzeit) geltenden aktuellen Rechts.

► Vorratsdaten als Zufallsfunde durften bis zum 02.03.2010 gemäß § 162 Abs. 2 StPO in andere Verfahren eingeführt werden, wenn für sie Schwellengleichheit bestand und in diesen Verfahren Vorratsdaten hätten erhoben werden dürfen.

► Seit dem 02.03.2010 dürfen Vorratsdaten als Zufallsfunde nicht mehr in andere Strafverfahren übernommen werden, weil § 100g StPO keine Schwellengleichheit zulässt.

► Vorhandene Vorratsdaten dürfen als Spurenansatz zur Begründung von Eingriffsmaßnahmen herangezogen werden. Als Vollbeweis sind sie ausgeschlossen.

► Dasselbe gilt wegen der Vorratsdaten, die zur Ergreifung des Täters benötigt werden. Sie dürfen verwendet werden.

Alle weiteren Einzelheiten und Belege ergeben sich aus dem Aufsatz über den

Umgang mit Verkehrsdaten.

Epilog

Den ganzen Januar 2010 habe ich darauf verwendet, eine Skimming-Anklage mit mehr als 1.800 Missbrauchstaten zu schreiben, wobei ich das Tagesgeschäft zurückgestellt habe. Die neue Rechtsprechung zum Skimming hat mich alle Freizeit aus dem Februar gekostet und die Entscheidung des BVerfG zur Vorratsdatenspeicherung das vollständige Wochenende, das heute

nach 11 Stunden Arbeit endet.

Ein Projekt wie der Cyberfahnder lässt sich auf dieser Grundlage nur begrenzt fortsetzen. Er lebt davon, dass ich nicht nur Neugier habe, sondern auch davon, dass mich solche Themen wie das Skimming und die Verwertbarkeit von Vorratsdaten beruflich ganz besonders interessieren.

Nötig wäre eine freigestellte Redaktion mit versierten juristischen Fachleuten, die zugleich auch IT-Sachverstand haben. Ihre Freistellung ist jedoch Illusion.

Ihr Cyberfahnder – Dieter Kochheim

Impressum