/ Veröffentlichung von IT-Sicherheitslücken: Full Disclosure vs. Responsible Disclosure

28.09.2018

Digital Business | Digital Business | Compliance & Interne Ermittlungen | Datenschutz | Datenschutz | IT & Outsourcing

Viele Softwareprodukte enthalten versteckte Programmfehler. Diese bergen ein immenses Sicherheitsrisiko, da sie Hackerangriffe und Systemmanipulationen ermöglichen. Das gilt insbesondere im vernetzten Internet of Things (IoT). Hier kann bereits ein einziger Klick genügen, um systemkritische Prozesse zu stören und globale Netzwerke vollständig lahmzulegen.

Softwarehersteller befinden sich in einem ständigen Wettlauf, bei dem es darum geht, Sicherheitslücken als erstes zu finden und schnellstmöglich per Updates zu schließen. Umso verheerender ist ein sog. **Full Disclosure**, bei dem ein Dritter eine Sicherheitslücke öffentlich bekanntgibt: Dies ruft Hacker auf den Plan, die binnen kurzem zum Cyber-Angriff blasen – vom Imageschaden des Softwareherstellers ganz zu schweigen.

Full Disclosure = Full Risk

Für die Entdecker einer Sicherheitslücke gilt die Faustregel: Full Disclosure = Full Risk. Denn die unbefugte Veröffentlichung eines Programmfehlers kann in vielerlei Hinsicht geltendes Recht verletzen. Je nach Einzelfall droht insbesondere ein Verstoß gegen Datenschutz-, Presse-, Wettbewerbsrecht. Häufig wird auch das Softurheberrecht verletzt, wenn mit dem Full Disclosure etwa eine Verletzungshandlung gemäß § 69c Nr. 1 bis 4 UrhG einhergeht. Zudem kann ein Full Disclosure die Täterschaft oder Teilnahme u.a. an folgenden Straftaten begründen: §§ 202a ff., 263a, 269 f., 303a f. StGB sowie § 17 UWG – insofern ist die Schwelle zum Cybercrime schnell überschritten.

Full Disclosures pro-aktiv verhindern

In jedem Fall sollten Softwarehersteller pro-aktiv sinnvolle Mechanismen vorsehen, um im Ernstfall sich anbahnende Full Disclosures rechtzeitig unterbinden und unkalkulierbare Folgeschäden verhindern zu können. Das gilt insbesondere, wenn Dritte Full Disclosures androhen, um wucherische Gegenleistungen zu erzwingen. Die Erfahrung zeigt, dass Softwarehersteller gut beraten sind, frühzeitig alle rechtlichen Optionen zu erwägen, um Full Disclosures zu verhindern und Nachahmer abzuschrecken. Je nach Einzelfall kommen u.a. neben Strafanzeigen urheber- und wettbewerbsrechtliche Abmahnungen und anschließend einstweilige Verfügungen sowie nachträgliche Schadensersatzklagen in Betracht.

Königsweg: Responsible Disclosure Agreement

Für Softwarehersteller besteht der Königsweg oft darin, den Entdecker der Sicherheitslücke – häufig gegen kleinere Belohnung (Stichwort: bug bounty program) – für ein sog. **Responsible Disclosure** zu gewinnen. Gemeint ist ein Verfahren, bei dem die Sicherheitslücke zunächst nur dem Softwarehersteller und erst später der Öffentlichkeit offenbart wird. Da das BGB (anders als beim Schatzfund) keinen bestimmten Anzeige- und Belohnungsmechanismus vorschreibt, ist umso wichtiger, die genauen Abläufe und Verschwiegenheiten verbindlich in Vertragsform festzulegen. Jedes Responsible Disclosure Agreements sollte unbedingt ausreichend flexible Fristenmechanismen vorsehen, damit dem Softwarehersteller genügend Zeit für die Behebung der konkreten Sicherheitslücke verbleibt.

Ausblick

Die Bedeutung von maßgeschneiderten Responsible Disclosure Agreements dürfte weiter steigen und auch zunehmend die Gerichte beschäftigen. Vor dem Landgericht Nürnberg-Fürth wurde jüngst nach fast sieben Stunden zäher Verhandlungen ein Responsible Disclosure Agreement geschlossen – vermutlich bundesweit zum allerersten Mal in Form eines gerichtlichen Vergleichs (Quelle: heise online news vom 06.09.2018). Nicht nur erkannte hier das Gericht explizit das Interesse des Softwareherstellers an, Sicherheitslücken eigenhändig und diskret schließen zu dürfen. Vielmehr hat das aktuelle Verfahren vor dem Landgericht Nürnberg-Fürth eines verdeutlicht: Im Ernstfall kann man mit umfassenden einstweiligen Verfügungen durchaus die nötige Verhandlungskulisse aufbauen, um die Entdecker einer Sicherheitslücke zum Abschluss eines Responsible Disclosure Agreements zu bewegen.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. David Bomhard
Practice Group: Digital Business

Contact Person

Dr. David Bomhard
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628 2610