ROMAN A. DICKMANN

Zusammenfassung

Regelung des behördlichen IT-Schwachstellenmanagements - Weniger IT-Schwachstellen als Staatsziel

Von Roman Dickmann und Dr. Oliver Vettermann, erschienen in der Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR, Beck Verlag), Heft 10/2022 vom 14.10.2022, Seiten 852-857

Im Anschluss an den Beitrag MMR 2022, 740 wird einleitend betont, dass es an einem staatlichen Prozess für den Umgang mit IT-Schwachstellen fehlt. Bislang wurde sich von Bund und Ländern nicht klar hinsichtlich des Umgangs mit ihnen positioniert. Daher muss damit gerechnet werden, dass Behörden gemeldete Schwachstellen für die Verwendung durch Sicherheitsbehörden geheimgehalten werden. Dies lässt bei den Melderinnen wenig Vertrauen aufkommen, zumal der Staat wie auch Kriminelle als Nachfrager am Schwachstellenmarkt auftreten, um von anhaltender IT-Unsicherheit zu profitieren. Zwischengeschaltet sind verstärkt Dienstleister, die Behörden etwa Trojaner-as-a-Service anbieten. Abhängigkeiten und Lock-In-Effekte sind die Folge in einer Beziehung, in der es an der nötigen Transparenz zur Überwachung der Dienstleister fehlt. Es werden deutlich die Gefahren der Geheimhaltung von Informationen zu Schwachstellen aufgezeigt, was durchaus für ein Verbot spricht. Abschließend findet sich ein Katalog zum gesetzlichen Mindestregelungsbedarf und die Forderung an die Gesetzgeber effektive ganzheitliche Lösungen zur Stärkung der IT-Sicherheit zu schaffen.

Executive Summary

Rules for a governmental IT vulnerability management - less IT vulnerabilities as national policy objective

citation of the original article: Dickmann/Vettermann MMR 2022, 852

authors: Roman Dickmann/Oliver Vettermann / journal: Zeitschrift für IT-Recht und Recht der Digitalisierung / Publisher: Beck / year: 2022 / issue: 10 / first page 852 (to 857)

With reference to MMR 2022, 740 the article begins with the missing governmental IT vulnerability management and no clear political position on the matter of secrecy versus disclosure. Finders of vulnerabilities have to fear that disclosures to governmental agencies will result in secrecy. This results in missing trust since the government (and likewise criminals) are the force behind market demand for new vulnerabilities to profit from the constant state of IT insecurity. Intermediaries for the government are service providers offering trojans-as-a-service. Dependencies and lock-in-effects are the consequences in a relationship without the necessary transparency for the agencies to control the service providers. The severe risks of secrecy are marked which arguments for a ban. The article finishes with a catalogue of specific topics for the legislators to regulate and a request for an effective holistic solution to strengthen IT security.

Rechtsanwalt Roman A. Dickmann · Taubenweg 4 · 61462 Königstein
LL.M. (Versicherungsrecht) · Europajurist (Univ. Würzburg) · Fachanwalt für Versicherungsrecht