FAQ zur E-Mail-/Telekommunikations-Überwachung und SINA

Warum werden Telefonate und E-Mails überwacht?

Zur Aufdeckung und Verhinderung von Straftaten sind bestimmte staatliche Stellen berechtigt, einzelne Bürger zu kontrollieren. Während sich dies in der Vergangenheit meist auf das Mitlesen von Briefen und das Abhören von Telefonaten oder Gesprächen beschränkte, erfolgt dies heute im Zeitalter der digitalen Kommunikation zunehmend über die Kontrolle von E-Mails oder sogar des gesamten Datenverkehrs über Internet und Mobiltelefon. In der Bundesrepublik Deutschland sind solche Maßnahmen ausschließlich mit einem richterlicher Beschluss zulässig, um Missbrauch oder unverhältnismäßige Maßnahmen zu verhindern.

Wie wird das Mitlesen von E-Mails geregelt?

Das Mitlesen von E-Mails durch staatliche Organe regelt die „Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation“ (kurz: Telekommunikations-Überwachungsverordnung, TKÜV). Die 2005 in Kraft gesetzte Verordnung wurde zuletzt am 25. Dezember 2008 aktualisiert.

Können Ermittler direkt auf E-Mails und andere Daten der überwachten Personen zugreifen?

Nein, die berechtigten Stellen[1] leiten eine Überwachungsanordnung an die E-Mail-Provider per Post oder per Fax weiter. Diese müssen sicherstellen, dass die entsprechend angeforderten Informationen in ihren Systemen identifizierbar sind. Anschließend leiten sie Kopien der angeforderten Daten verschlüsselt über die SINA Infrastruktur an die berechtigten Stellen weiter.

Welche Funktion hat SINA dabei?

SINA (Sichere Inter-Netzwerk Architektur) sichert den Austausch von Daten zwischen den berechtigten staatlichen Stellen und den verpflichteten Telekommunikationsanbietern. Dabei dient SINA (konkret: die SINA Box) ausschließlich der Verschlüsselung und Absicherung des Datenverkehrs vor unbefugter Einsichtnahme. SINA enthält keine Funktionalität zum Auslesen oder zum Auswerten von E-Mails. Zudem hat der Hersteller secunet Security Networks AG keinen Zugriff auf die Bedienung und Verwaltung des Geräts im laufenden Betrieb.

[1] * Begriffsbestimmung gem. TKÜV §2: „Im Sinne dieser Verordnung […] die nach § 100b Abs. 3 Satz 1 der Strafprozessordnung, § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes, § 23a Abs. 1 Satz 1 des Zollfahndungsdienstgesetzes oder nach Landesrecht auf Grund der jeweiligen Anordnung zur Überwachung und Aufzeichnung der Telekommunikation berechtigte Stelle […].“

Können staatliche Stellen über SINA Spionage-Software wie den „Bundestrojaner“ installieren?

Nein, SINA ist in keiner Weise in den Datenverkehr zwischen Endanwender und Anbieter oder zwischen Endanwender und staatlicher Stelle involviert. Daher müsste eine Überwachungssoftware wie der so genannte „Bundestrojaner“ auf andere Weise auf einem Endgerät installiert werden.
SINA besitzt auch keine Funktionen, um Daten in unsicheren Netzen abzuhören, zu verändern oder zu manipulieren. SINA hat stattdessen genau die entgegen gesetzte Funktion, nämlich den Datentransfer zwischen Telekommunikationsanbietern und berechtigten Stellen abzusichern und vor unberechtigtem Zugriff zu schützen.

Wer hat Zugriff auf die Konfiguration der SINA Boxen?

Die Bundesnetzagentur konfiguriert als unabhängige Instanz die im Rahmen von TKÜ eingesetzten SINA Boxen. Die Bundesnetzagentur hat jedoch anschließend keinen Zugriff auf die übermittelten Daten oder die Verwaltung von SINA im laufenden Betrieb. Die Systeme zum Auslesen der Informationen beim Anbieter sowie zur Auswertung bei den staatlichen Stellen sind unabhängig von SINA.

Müssen E-Mail-Provider SINA Boxen integrieren?

Anbieter müssen eine sichere Infrastruktur zur Datenübertragung an die berechtigten Stellen vorhalten, andernfalls drohen ihnen Bußgelder oder sogar der Lizenzentzug, da sie richterliche Beschlüsse nicht umsetzen können. Kleinere E-Mail-Provider ohne eigene sichere Infrastruktur zur Datenübertragung können jedoch auf Dienstleister zurückgreifen, die eine solche sichere Infrastruktur bereitstellen.

Warum kommt SINA zum Einsatz?

Die „Sichere Inter-Netzwerk Architektur“ SINA hat secunet im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelt. Sie wurde vom BSI als hochsichere Architektur zur Übertragung sensibler Daten über unsichere Netze, vor allem dem Internet, für die Behörden der Bundesrepublik Deutschland zugelassen. SINA wird in verschiedenen Anwendungsszenarien in Unternehmen sowie Behörden mit unterschiedlichen Sicherheitsanforderungen verwendet.

((4.148 Zeichen))

Pressekontakt:

Patrick Franitza
Stellv. Pressesprecher

secunet Security Networks AG
Kurfürstenstr. 58
45128 Essen/Germany
Tel.: +49 201 5454-1234
Fax: +49 201 5454-1235
E-Mail: presse@secunet.com
http://www.secunet.com