Anlass: Meldung vom 17. September 2019	Experte für Verschlüsselung:
Patientendaten: **Millionen Daten ungeschützt im Netz**	**Robert Freudenreich,** **CTO bei Boxcryptor | Secomba GmbH**

Statement: Patientendaten öffentlich einsehbar

Wie der Bayerische Rundfunk in Zusammenarbeit mit ProPublica herausgefunden hat, liegen **Millionen Patientendaten frei abrufbar** im Netz. Zu diesem Sachverhalt möchten wir ein Statement abgeben.

Robert Freudenreich, CTO von Boxcryptor, Verschlüsselungssoftware aus Augsburg

Mit Bestürzen lesen wir wieder einmal von veröffentlichten Daten mit hochsensiblen Inhalten. Wieder einmal wäre ein Datenleck vermeidbar gewesen. Es wird Zeit für einen Paradigmenwechsel:

„Wir müssen wegkommen, die Codezentrische Sicherheit als Lösung zu betrachten. Das Ziel muss flächendeckende Datenzentrische Sicherheit durch starke Verschlüsselung sein.“

Zur Erläuterung: Wenn es darum geht, sensible Daten zu schützen, gibt es zwei unterschiedliche Herangehensweisen, die bereits im Aufbau der Software implementiert werden.

- Ein häufig angewendetes (und fehleranfälliges) Verfahren ist die **Codezentrische Datensicherheit**. Dabei sind die Daten prinzipiell für jeden lesbar. Durch Zugriffskontrollen im Programmcode (bspw. Zugriffsberechtigung) werden die Daten geschützt. Unbefugte können gezielt nach Fehlern bei der Zugriffskontrolle suchen oder die Konfiguration ausnutzen, um Zugriff auf Daten zu erlangen. Dies war beim aktuellen Fall der veröffentlichten Patientendaten die Ursache des Datenlecks. Stellen Sie sich einen Türsteher vor dem Club vor, der mit Augenaufschlag, Bestechung oder einem gut platzierten Faustschlag zu überwinden ist.
- Die andere, von mir bevorzugte, Herangehensweise ist die **Datenzentrische Sicherheit**. Die Daten selbst werden durch Verfahren wie Verschlüsselung direkt geschützt und Zugriffe sind ausschließlich mit Besitz des entsprechenden Schlüssels möglich. Unbefugte können keine Fehler im Programm ausnutzen um unberechtigten Zugriff auf die somit geschützten Daten zu erlangen. Diese Tür ist nicht mit einem Türsteher geschützt, sondern mit einem Schloss – ohne passenden Schlüssel kein Einlass.

Das grundlegende Problem dafür, dass wir – trotz Inkrafttreten der DSG-VO noch immer keine flächendeckende Verschlüsselung sensibler und besonders schützenswerter Daten haben, liegt meiner Meinung nach an der schwammigen Formulierung von Artikel 32 DSG-VO, indem lediglich von „geeigneten technischen und organisatorischen Maßnahmen“ zum

Schutz der Daten gesprochen wird. Hier bietet das Regelwerk meiner Ansicht nach zu viel Interpretationsspielraum – zu Lasten der Betroffenen. Die Pflicht zur Verschlüsselung von besonders schützenswerten Daten ist für mich alternativlos.

Heute sind es Millionen Patienten weltweit, gestern war es die komplette Bevölkerung Ecuadors – wir können nicht weiterhin so leichtfertig mit unseren sensibelsten Informationen umgehen!

Ihre Ansprechpartnerin für Nachfragen:

Secomba GmbH
Lisa Figas
Werner-von-Siemens-Str. 6
86159 Augsburg

www.boxcryptor.com
tel: +49 (0821) 907 861 57
fax: +49 (0821) 907 861 59
mail: lf@secomba.com

Über Boxcryptor
Die Secomba GmbH ist ein deutsches Unternehmen und Hersteller von Boxcryptor, einer Cloud-optimierten Verschlüsselungslösung für Unternehmen und Privatpersonen. Das Unternehmen wurde 2011 von Andrea Pfundmeier und Robert Freudenreich gegründet. Boxcryptors integrierte Zero-Knowledge- und Ende-zu-Ende-Verschlüsselung schützt Daten in der Cloud vor unberechtigtem Zugriff und ermöglicht somit die sichere Nutzung zahlreicher Cloud-Dienste. Boxcryptor wird von führenden Unternehmen sowohl in Europa als auch weltweit zur sicheren Kollaboration in der Cloud genutzt. Erfahren Sie mehr auf www.boxcryptor.com.