Occasion: Message of 17 September 2019 **Patient records:** **Millions of data unprotected on the net**	Encryption Expert: **Robert Freudenreich,** **CTO at Boxcryptor | Secomba GmbH**

Statement: Patient Data Publicly Accessible

As the Bayerischer Rundfunk in cooperation with ProPublica has found out, **millions of patient data** are freely available on the net. We would like to make a statement on this issue.

Robert Freudenreich, CTO of Boxcryptor,
Encryption software from Augsburg, Germany

With dismay we read once again from published data with highly sensitive contents. Once more, a data leak would have been avoidable. It's time for a paradigm shift:

"We must get away from seeing code-centric security as a solution. The goal must be to provide comprehensive data-centric security through strong encryption."

Explanation: When it comes to protecting sensitive data, there are two different approaches that are already implemented in the structure of the software.

- **Code-centric data security** is a frequently used (and error-prone) procedure. In principle, the data can be read by anyone. The data is protected by access controls in the program code (e.g. access authorization). Unauthorized persons can specifically search for errors in access control or use the configuration to gain access to data. This was the cause of the data leak in the current case of published patient data. Imagine a bouncer in front of the club who can be overcome with a look, a bribe or a well-placed punch.

- The other approach, I strongly prefer, is **data-centric security**. The data itself is directly protected by procedures such as encryption and accessing the data is only possible with the appropriate key. Unauthorized persons cannot take advantage of errors in the program to gain unauthorized access to the protected data. This door is not protected with a bouncer, but with a lock - without a suitable key, there can be no admission.

In my opinion, the fundamental problem for the fact that we still do not have nationwide encryption of sensitive and particularly sensitive data - despite the commencement of the GDPR - is the vague wording of Article 32 of the GDPR, in which the term "appropriate technical and organizational measures" for data protection is used. In my opinion, the body

of rules offers too much room for interpretation here - to the detriment of those affected. The obligation to encrypt particularly sensitive data has no alternative for me.
Today, this affected millions of patients worldwide, yesterday, the entire population of Ecuador was affected – we cannot continue to deal so imprudent with our most sensitive information!

Your contact for inquiries:

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

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

About Boxcryptor
Secomba GmbH is a German company and manufacturer of Boxcryptor, a cloud-optimized encryption solution for companies and private individuals. The company was founded in 2011 by Andrea Pfundmeier and Robert Freudenreich. Boxcryptor's integrated zero-knowledge and end-to-end encryption protects data in the cloud from unauthorized access and thus enables the secure use of numerous cloud services. Boxcryptor is used by leading companies both in Europe and worldwide for secure collaboration in the cloud. Learn more at www.boxcryptor.com.