Date: *January 01, 2019*
Source: *datensicherheit.de*
https://www.datensicherheit.de/aktuelles/gesundheits-apps-sicherheitsluecke-kann-geschlossen-werden-29644

Press Report

Health-Apps: Safety-gap can be closed

Dr. Florian Scheuer comments hacker-attack against „Vivy“ and shows way forward

After the attention around the hacker-attack against the health-file-app *Vivy* apparently died down over the last few weeks, it was an intensively discussed topic at the „Chaos Communication Congress“ (35C3) in Leipzig, according to Dr. Florian Scheuer. The reason was the **detailed description of the safety-gaps** in the talk given by the discoverer, Martin Tschirsich. Once again it became clear, which fundamental mistakes were made during the well-financed development of the app *“that claims to offer ‘highest security levels’ according to their website”*, comments Dr. Scheuer.

Weak safety measures for critical patient data

It seemed especially problematic that the weak security measures protecting critical patient data could be **easily overcome** with only a few tries.
Furthermore, it was possible to plant **phishing-attacks** within the app. Thus, access data of users could be stolen (without a chance of detection) and a way to steal sensitive cryptographic keys from doctors presented itself. Dr. Scheuer: *“Especially the last safety-gap has not been closed until today.”*

Weak security for secret cryptographic keys

However, not only *Vivy* seems to be affected by serious security and data safety problems: Tschirsich also analysed the alternatives by large and small providers and found severe problems there too. Some even enabling **access to all data** of the system.
The by far the best performing app (“TK Safe”) was still in its beta-phase; it ensured safety of health data through client-side encryption. Here, the data is supposed to already be strongly encrypted within the app. Only afterwards, it is transferred to the central server or exchanged with a recipient (e.g. attending physician). Nevertheless, *“even here serious mistakes were made in securing the secret cryptographic keys”* Dr. Scheuer reports.

Client-side encryption recommended

These implementation problems showed that security standards need to already be taken into account **from the beginning** of the development of these critical systems and deeply embedded within the software-architecture. Adding security measures later is *“often difficult and prone to error”*.

Furthermore, **only client-side encryption** could really prevent data from falling into the hands of an attacker in case of an information leakage, Dr. Scheuer emphasises.

According to its information DRACOON is a provider of an enterprise-filesharing-solution for the management of sensitive information with **multiple security mechanisms**. Already today many clinics in the healthcare sector are *“successfully using this solution and therefore protecting sensitive information of many patients in Germany”.*