Der Heartbleed-Bug

Manche haben vielleicht davon gelesen. Gestern, am 8. April 2014 wurde eine Sicherheitslücke in einer Softwarkomponente bekannt, die quasi eines der Herzstücke der Sicherheitsarchitektur des Internets betrifft.

Die Programmbibliothek openssl, die viele Programme zum Verschlüsseln von Daten nutzen hatte in ihrer aktuellen Version einen Programmierfehler, der es ermöglichte, den geheimen Schlüssel vom Server auszulesen.

Eingesetzt wird openssl z.B. bei verschlüsselten Webseiten (https:*) Ein Angreifer, dem das gelingt, kann in der Folge, sofern er/sie Zugriff auf den Datenstrom hat auch alle verschlüsselte Kommunikation mitlesen. Im schlimmsten Fall sogar, wenn die sogenannte secret forwarcy nicht aktiviert war, können auch in der Vergangenheit aufgezeichnete Daten entschlüsselt werden.*

From:
https://wiki.datenkollektiv.net/ - **datenkollektiv.net**

Permanent link:
https://wiki.datenkollektiv.net/info_zum_heartblead-bug?rev=1397035217

Last update: **2014/04/09 11:20**