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. (Siehe z.B. Artikel auf heise.de)

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 auf dem Server die sogenannte Forward Secrecy nicht aktiviert war (bzw. z.B. der Webbrowser dies nicht unterstützt hat), können auch in der Vergangenheit aufgezeichnete Daten entschlüsselt werden.

notraces.net nicht betroffen

Die gute Nachricht: Der Mailserver von notraces.net war nicht betroffen, da er eine openssl-Version einsetzte, die diese Sicherheitslücke nicht besitzt.

Die schlechte Nachricht für uns war: wir haben gestern alle unsere neu generierten Zertifikate auf den neuen Servern noch einmal ausgetauscht. Unsere Server waren zwar bislang nur zu Testzwecken am Netz. Aber wir wollten kein Risiko eingehen - sei es auch noch so unwahrscheinlich.

Daher haben sich nun unsere Zertifikate - und auch die abgeleiteten „Fingerabdrücke“ geändert und sind jetzt nicht mehr die, die wir euch in der ersten E-Mail zur Umzugsankündigung genannt haben.