

Verschlüsselte auslesen?

E-Mails

[Tagesschau](#): „Die neuen Erkenntnisse zu den Anstrengungen von NSA und GCHQ bedeuten nicht zwangsläufig, dass die Geheimdienste alle verschlüsselten Mails auslesen. Sie haben nach Ansicht von Experten dadurch in Verdachtsfällen die Möglichkeit jede E-Mail zu knacken – sollten die Angaben Snowdens der Wahrheit entsprechen.“ (Danke, [Ruben](#): „Was berichten die Medien als Nächstes? Das Gerät NSA kann jetzt alles, auch Kaffee kochen?“)

Was ist denn das für ein Unsinn? Und welche „Experten“ wurden da gefragt?

Gestern zitierte ich Edward Snowden. u.a. laut [Wired](#):

Properly implemented strong crypto systems are one of the few things that you can rely on,” he said, though cautioning that the N.S.A. often bypasses the encryption altogether by targeting the computers at one end or the other and grabbing text before it is encrypted or after it is decrypted.

[Heise](#) übersetzt das so: „Verschlüsselung funktioniert. Sauber implementierte, starke Verschlüsselung ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“ Die Betonung liegt auf „sauber implementiert“.

Wie ich immer in meinen Seminaren sage: Man kann sich das Niveau der Berichterstattung deutscher Medien über Sicherheitsthemen nicht unterirdisch genau vorstellen.