Warum existieren die DNSSEC-Erweiterungen?

Das DNS-System ohne DNSSEC besitzt die beiden o.g. Sicherheitsmerkmale (Quellenauthentifizierung und Datenintegrität) nicht. Es gibt zwar rudimentäre Verfahren um möglichst sicherzustellen, dass Nameserver auf ihre Anfragen eine authentische Antwort erhalten, allerdings ist deren Wirksamkeit mindestens seit Bekanntwerden der [Kaminski-Attacke] überaus fraglich. Zwar wurden die entsprechenden Verfahren (Zufalls-Query-IDs und Zufalls-Anfrage-Portnummer) verstärkt, so dass die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert wird, allerdings bietet nur eine digitale Signatur der Daten einen theoretisch fundierten und ausreichend sicheren Schutz. Die genaue Funktionsweise und die Hintergründe von Kaminskis DNS-Angriff sind beispielsweise unter http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html umfassend dargestellt.

Weitere Informationen:

- http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Eindeutige ID: #1001
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:33