

Computerworld.ch

Schweizer Krypto-Spezialist expandiert

Der Schweizer Verschlüsselungs-Spezialist Barclay Technologies hat mit dem Reseller ADN Distribution auch ein Standbein in Deutschland und Österreich erhalten. Zudem werden die Aktien der Firma auch an der Frankfurter Börse gehandelt.

(ist)



Mit ADN besitzt die in Urdorf ansässige Barclay Technologies einen gemeinsamen Vertriebskanal für ihr Verschlüsselungsprodukt Certus Lateo für Deutschland, Österreich und die Schweiz. Auch der Frankfurter Börsengang dürfte dem Unternehmen bei der Expansion behilflich sein und Mittel in die Kasse spülen.

Certus Lateo (Latein für "ich verberge sicher") basiert auf einer neuartigen Verschlüsselungstechnik, die ursprünglich vom Firmengründer und heutigem CEO Freddy Zähler ausgeheckt wurde. Für eine Echtzeit-Handelsplattform und für die Errichtung eines Online-Kasinos musste er ein Verschlüsselungsverfahren verwenden, das sozusagen in Echtzeit chiffriert und dechiffriert sowie kaum zusätzliche Bandbreite beansprucht.

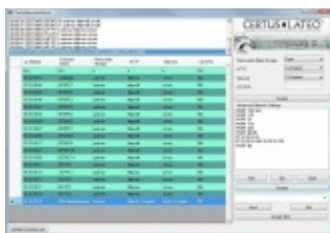


Kilian Zantop, CTO von Barclay Technologies

Wie Kilian Zantop, CTO von Barclay Technologies, gegenüber Computerworld.ch ausführt, werde bei dem Verfahren jedes einzelne Paket verschlüsselt, wobei das verschlüsselte Paket quasi die selbe Grösse aufweist wie das Ursprungspaket. "Es entsteht also kein Overhead, und die Übertragung benötigt keine zusätzliche Bandbreite wie der Versand der unverschlüsselten Informationen".

Dies ist laut Zantop möglich weil sich das Verfahren vom Prinzip her einer Art Ersetzungsalgorithmus bedient. Zudem weist es Elemente eines symmetrischen Verschlüsselungsverfahrens auf, mit dem Unterschied, dass der Schlüssel nicht getauscht wird. "Es gibt keinen Schlüsselaustausch, kein Keymanagement und keinen Handshake", führt er weiter aus.

Vielmehr spürt die Empfängerseite anhand gewisser Indizien im unverschlüsselten Header auf, wo im verschlüsselten Paket sich weitere Hinweise auf den Schlüssel befinden. Dieser wurde zuvor vom Sender verwendet, nach Gebrauch aber weggeworfen. Die Indizien wiederum erhält die Gegenstelle aufgrund der gemeinsamen Kommunikationsgeschichte von Sender und Empfänger.



Das Administrationstool von Certus Lateo

Um das Ganze noch etwas sicherer zu machen, werden die einzelnen Pakete mit mehreren, jeweils unterschiedlichen Algorithmen verschlüsselt, wobei zudem verschiedene Schlüsseltiefen verwendet werden.

Dadurch, dass eigentlich nur der Empfänger den Schlüssel rekonstruieren kann und dass jedes Paket anders verschlüsselt wird, sei es praktisch nicht möglich, die Informationen zu dechiffrieren. "Ich habe mir lange Gedanken darüber gemacht, wie

man das knacken könnte, komme aber auf keine Lösung", meint Zantop. Selbst Barclay Technologies als Hersteller des Verfahren habe keine Möglichkeit, den Schlüssel herauszufinden.

Doch Certus Lateo lässt sich nicht nur zur Codierung von Netzwerkverkehr einsetzen, es kann auch den Datentransfer auf Speichermedien wie USB-Sticks und DVDs regulieren. Es eignet sich somit auch zur Data Leakage Prevention ([\[1\] vgl. hierzu den ausführlichen Computerworld.ch-Artikel "Schweizer Software verhindert Datenklau"](#)).

Enthaltene Links:

[1] <http://www.computerworld.ch/aktuell/news/48137/index.html>