AES-VPN
mit hochsicherem, automatisiertem Schlüsseltausch

Eine Besonderheit des von der AVI Security entwickelten AES-VPN, ist der hochsichere, vollautomatisierte, mehrfach verschlüsselte, zeitlich frei wählbare Schlüsseltausch. Während bei den uns bekannten VPN Anbietern jeweils nur einmal ein Schlüssel generiert wird um die Verbindung zu sichern, gibt es beim AES-VPN einen Dienst welcher mit einer AES-256-Bit Verschlüsselung z.B. täglich alle Schlüssel automatisch tauscht. Nur der zum VPN-Server passende VPN-Client, kann in Kombination mit dem richtigen Benutzer Account die Schlüssel verwenden. Das bedeutet für einen Angreifer, dass er in diesem Fall lediglich 24h Zeit hat um den jeweiligen Schlüssel zu knacken, vorausgesetzt er hat einen gültigen Account. Derzeit wird bei einer AES Verschlüsselung von folgenden Zeiten zum knacken ausgegangen:

Schlüssellänge	**Zeit, alle Kombinationen zu versuchen**
56-Bit AES-Verschlüsselung	399 Sekunden
128-Bit AES-Verschlüsselung	$1{,}02 * 10^{18}$ Jahre
192-Bit AES-Verschlüsselung	$1{,}872 * 10^{37}$ Jahre
256-Bit AES-Verschlüsselung	$3{,}31 * 10^{56}$ Jahre

Quelle: https://www.passwort-generator.com/aes-verschluesselung/

Die in der Tabelle angegeben Werte sind natürlich relativ. Es gibt verschieden Faktoren wie z.B. Zugriffszeiten und Rechnenpower welche die in der Tabelle angegebenen Zeiten beeinflussen. Trotzdem ist klar, umso weniger Zeit ein Angreifer hat um einen Schlüssel zu knacken, desto exponentiell höher ist der Schwierigkeitsgrad und damit der Aufwand.

AVI Security GmbH
Parchimer Str. 25
22143 Hamburg
Tel.: 0049 40 5326 2503
Web: www.avi-security.de
E-Mail: info@avi-security.de