Daten verschlüsseln

Thomas Engel (Text und Bild)

Immer öfter verlassen Daten unseren PC, als E-Mail, via FDP, auf einer CD gebrannt, im USB-Stick gespeichert oder übers Internet. Leider gelangen diese Daten nicht immer dorthin, wo wir es möchten. Sie gehen verloren, werden gestohlen oder ausspioniert.
In mehreren Beiträgen habe ich über Datensicherheit im Sinn von Backups gesprochen. Leider erfahre ich immer wieder von Personen, dass sie ihre Daten: Bilder, Texte usw. wegen eines Harddisk-Crashs oder wegen Verlust des Laptops nicht mehr besitzen. Ein ganz anderes Thema ist jedoch die Datensicherheit im Sinne des Datenschutzes. Da wir Zahnärzte mit persönlichen Patientendaten arbeiten, sollten wir das Thema Datenschutz besonders gut beachten. Heutige USB-Sticks haben oft 32, 64 oder 128 GB Speicherkapazität und fassen unglaubliche Datenmengen. Es ist ganz einfach, sämtliche Patientenfotos der eigenen Praxis immer auf einem Speicherstick bei sich zu haben. Verlieren wir das Speichermedium oder wird es gar gestohlen, verlieren wir die Kontrolle über die gespeicherten Daten. Heute gibt es spezielle Verschlüsselungsprogramme, welche ganze «Datencontainer» verschlüsselt anlegen können und es fast unmöglich machen, diese Daten ohne entsprechendes Passwort zu lesen. Gehen die Daten verloren und geraten in falsche Hände, können wir relativ sicher sein, dass diese nicht gelesen werden können. Können wir glaubhaft belegen, dass die heiklen Daten verschlüsselt waren, verleiht uns dies Rechtssicherheit.
Ein Gratis-Verschlüsselungsprogramm ist z. B. «True Crypt». Es läuft sowohl auf Windows und Mac als auch auf Linux-Rechnern.

Verschlüsselung

AES: Advanced Encryption Standard ist ein symmetrischer Verschlüsselungsstandard. Symmetrisch bedeutet, dass sowohl beim Verschlüsseln als auch beim Entschlüsseln das gleiche Passwort benutzt wird.
Der AES-Logarithmus kann mit einer Blockgrösse von 128 Bit und einer Schlüssellänge von 128, 192 oder 256 Bit verwendet werden und bietet ein hohes Mass an Sicherheit. Da der Algorithmus frei ist, darf er ohne Lizenzgebühren verwendet werden.
Bei der Verschlüsselung werden die Daten in Blöcke unterteilt und jeder Block wird einzeln verschlüsselt. Dabei durchläuft jeder Block mehrere Verschlüsselungsrunden.
Twofish: Auch Twofish ist ein symmetrischer Verschlüsselungsalgorithmus. Es handelt sich um einen Block-Cipher mit einer Blockgrösse von 128 Bit und 16 Runden, die Schlüssellängen betragen 128, 192 oder 256 Bit.
Ähnlich wie bei der AES-Verschlüsselung werden die einzelnen Blöcke durch mehrmalige gegenseitige XOR-Verknüpfungen verschlüsselt.
Serpent: Wie die beiden bereits beschriebenen Verschlüsselungsverfahren ist auch Serpent eine symmetrische Blockverschlüsselung.
Serpent gilt als sehr sichere Verschlüsselungsmethode, welche jedoch relativ langsam ist. So wird sie oft in hardwarebasierten Verschlüsselungstechnologien und weniger in softwarebasierten Verfahren angewendet.
True Crypt beherrscht alle drei Verschlüsselungsverfahren und kann diese auch kombinieren. Es gibt noch weitere Programme, Twofish, Serpent und True Crypt gehören jedoch zu den bekanntesten und sichersten und werden viel gebraucht.

Es gibt Onlinespeicher, welche die Daten vor dem Upload auf dem eigenen Rechner entsprechend verschlüsseln und damit die Daten sicher vor unberechtigtem Zugriff speichern. Ein solcher Onlinespeicher ist z. B. der an der ETH entwickelte Dienst «Wuala».

Schwachstellen

Die genannten Verfahren sind derart sicher, dass bis heute keine Attacke bekannt ist. Das grösste Gefahrenpotenzial besteht beim Benutzer. Auch das beste Verschlüsselungsprogramm nützt nichts, wenn das Passwort zu schwach oder dieses aufgeschrieben wird. Die meisten bekannten Attacken – auch erfolgreiche – zielen deshalb direkt auf das Passwort. Mit dem gestohlenen Passwort können die Daten dann entschlüsselt werden.
Es gibt heute zahlreiche Spionagesoftwares, welche nur diesen Zweck verfolgen und alle Tastenanschläge speichern und dem «Spion» mitteilen.
Wird die Verschlüsselungssoftware nicht mehr unterhalten, steht sie für neue Betriebssysteme nicht mehr zur Verfügung. Somit könnten ältere verschlüsselte Daten nicht mehr zurück entschlüsselt werden.
Gefährlich ist auch der Verlust des Passwortes: Einmal verschlüsselte Daten sind so sicher, dass sie sich ohne entsprechendes Passwort nicht mehr wiederherstellen lassen.

Fortsetzung folgt …