AuthCryptor

Höchster Schutz für Passwort und Daten
auf allen Kommunikations- und Übertragungswegen

SDT-Solutions

AuthCryptor steht für umfassende Datensicherheit

Heutzutage erfordert jede Datenübertragung ein Passwort zur Anmeldung. Ob Onlinebanking, Austausch von oder Zugriff auf wichtige Unternehmensdaten, Steuerung von Industrieanlagen, Abruf vertraulicher Dokumente wie Patientenakten oder das Management des Smart Homes – allerorts sind Authentifizierungen, also Nachweise der Identität von Benutzern mittels Passwort, die gängige Methode für die Kommunikation zwischen Client und Datenservern. VPN-Verbindungen, Zertifikate oder Sicherheits-Apps schützen aktuell noch solche Vorgänge. Dennoch registriert das Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zu 39.000 Infektionen deutscher IT-Systeme am Tag. Die Zahlen zeigen: Der heutige Sicherheitsstandard reicht nicht aus.

Insider oder Man-in-the-Middle: Keine Chance für unautorisierten Zugriff

Übliche Verfahren für die Anmeldung auf einem Server überprüfen die Identität des Servers mithilfe eines Zertifikats. Die Identität des Nutzers wird durch Passwortkenntnis bestätigt. Ein Risiko besteht darin, dass ein an den Server gesendetes Passwort von einem Innentäter mitgeschnitten wird. Ein solcher «Insider»-Angriff kann auch ungewollt durch infizierte Laptops, USB-Sticks oder mobile Endgeräte von Mitarbeitern erfolgen.

Eine weitere Gefahr herkömmlicher Verfahren ist, dass sich zwischen die Verbindung von Nutzer und Datenserver ein sogenannter «Man-in-the-Middle» (MitM) aufschaltet, sie belauscht oder manipuliert. Passwörter werden ausgespäht und unberechtigt verwendet. Der Benutzer bemerkt davon nichts und auch für den Server ist die unberechtigte Authentifizierung ein stimmiger Vorgang. Sowohl Insider- als auch MitM-Angriffe haben weitreichende Folgen: Unbefugte erhalten Datenzugriff und können Vorgänge anstoßen. Das Gefahrenpotential ist enorm und wird von vielen Anwendern unterschätzt.

AuthCryptor im Überblick

- Insider-Angriffe, bewusst oder unbewusst, werden abgewehrt
- Man-in-the-Middle-Angriffe werden verhindert
- Höchster Passwortschutz: keine Speicherung oder Übertragung von Passworten oder passwortäquivalenten Daten
- Authentifizierung und Verschlüsselung werden zu einem Verfahren verknüpft
- Integrität, Herkunft und Vertraulichkeit aller Daten wird durch Ende-zu-Ende-Verschlüsselung gewährleistet
- Höchst sichere, verschlüsselte Datenübermittlung auch in offenen Netzen, bei gleichzeitiger Unabhängigkeit von Dritten, wie der öffentlichen Zertifikatsinfrastruktur
- Mehrere Netzwerkdienste können zu einer Verbindung gebündelt werden. Das notwendige interne Routing wird von AuthCryptor übernommen. Die Anzahl nach außen offener Ports kann somit auf einen einzigen reduziert werden.
- Die Eigenschaft der «Perfect Forward Secrecy» wird erfüllt, das heißt für jede Verbindung wird ein neuer, unabhängiger Sitzungsschlüssel generiert
- Kein Absetzen falscher Statusmeldungen seitens unberechtigter Dritter möglich
- Kundenfreundlichkeit und einfache Bedienung über jegliche Endgeräte
- Den Empfehlungen und Richtlinien des BSI und der NIST wird Folge geleistet
- In bereits bestehende Netze nachrüstbar

Neue Ansätze für zukünftige Herausforderungen

Mit AuthCryptor geht kein Passwort verloren. Es wird bei der Anmeldung auf einem Server nicht übertragen und kann somit auch nicht gestohlen werden. Jede Passworteingabe löst stattdessen immer eine neue und unabhängige Schlüsselberechnung aus. Das Funktionsprinzip beruht auf mathematischen Berechnungen, die von Client und Server für jede Authentifizierung durchgeführt werden. Nur passende Gegenstücke und deren Kombination erkennt das System als berechtigt an. Unbefugte Dritte können zu keinem Zeitpunkt ein Passwort oder passwortäquivalente Daten abgreifen, da diese weder gespeichert noch übertragen werden. Selbst ein gekaperter Sitzungsschlüssel gibt keine Hinweise auf vergangene oder zukünftige Schlüssel. Das macht AuthCryptor zum zuverlässigen Torwächter.

Benutzerfreundlichkeit und Mobilität

Für den Nutzer ist die Authentifizierung mit AuthCryptor einfach: Er gibt wie gewohnt sein Passwort ein. Auch über mobile Endgeräte und in unsicheren Netzwerken wird niemals ein Kennwort übertragen.

Datensicherheit auf höchster Stufe

Mit AuthCryptor existiert eine sichere, zum Patent angemeldete und den Richtlinien des BSI und der NIST folgenden Authentifizierungslösung, die gleichzeitig Herkunft, Integrität und Vertraulichkeit der versandten Daten durch eine Ende-zu-Ende-Verschlüsselung zwischen beteiligten Kommunikationspartnern gewährleistet. Sensible Daten werden weder gespeichert noch übertragen. Das Ergebnis: Insider- und MitM-Angriffe sind zwecklos.

SDT-Solutions

SDT-Solutions GmbH
Erb 10 · D-77876 Kappelrodeck
Telefon: +49 7842 98856
E-Mail: info@sdt-solutions.de
www.sdt-solutions.de