15.01.2020

Presseinformation

Vertraulichkeit und Integrität für alle Daten

AuthCryptor schließt Einfallstore in Kommunikations- und Übertragungswege mit patentiertem Verfahren

Höchster Schutz für Passwort und Daten auf Kommunikations- und Übertragungswegen – in Zeiten der Digitalisierung ist das von oberster Priorität. Hierbei gilt: Am sichersten ist der Schlüssel, der weder gespeichert noch übertragen wird. Dieses Prinzip dient der SDT-Solutions GmbH als Grundlage für ihre neuartige, patentierte Authentifizierungsmethode mit integrierter Ende-zu-Ende-Verschlüsselung. Mit ihrer Authentifizierungssoftware AuthCryptor gehen keine Daten mehr verloren. Jeder Verbindungsaufbau löst eine neue und unabhängige, asymmetrische Schlüsselberechnung aus.

Cybersicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung. Unternehmen jeder Größenordnung, Banken, Ärzte, Rechtsanwälte aber auch Privatpersonen beim Homebanking oder im Smart Home müssen sich vor Cyberattacken schützen. Knapp 70 Prozent der Unternehmen und Institutionen in Deutschland sind laut BSI[1] in den Jahren 2016 und 2017 Opfer von Cyberangriffen geworden. Die Folge: manipulierte IT-Systeme und Internetauftritte, Produktions- und Betriebsausfälle, Imageverlust und hohe Kosten für Aufklärung und Wiederherstellung der Systeme.

1 Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Gefaehrdungslage/Lageberichte/cs_Lageberichte_node.html, Seite 15 (abgerufen am 18.09.2019)

Man-in-the-Middle und Insider-Angriff bei Punkt-zu-Punkt-Kommunikation und Authentifizierungsvorgängen

Die Schwachstelle liegt in den Authentifizierungsvorgängen. Übliche Verfahren überprüfen die Identität des Servers mithilfe eines Zertifikats. Die Nutzer-Identität wird durch Passwortkenntnis bestätigt. Ein gesendetes Passwort kann allerdings von einem Innentäter mitgeschnitten werden. Ein Insider-Angriff kann auch durch infizierte Laptops, USB-Sticks oder mobile Endgeräte ungewollt durch Mitarbeiter erfolgen. Eine weitere Gefahr herkömmlicher Verfahren ist, dass sich zwischen die Verbindung von Nutzer und Datenserver unbemerkt ein sogenannter „Man-in-the-Middle“ (MitM) aufschaltet, sie belauscht oder manipuliert. Für den Server ist der zwischengeschaltete MitM nicht zu erkennen und es findet ein vermeintlich stimmiger Vorgang statt. Für Datenschützer ist die Lage allerdings noch komplizierter, wenn statt einer Punkt-zu-Punkt-Kommunikation ein zentraler Punkt inkludiert ist, über den Daten fließen. Typische Netzwerkinfrastrukturen bestehen aus einem zentralen Punkt, beispielsweise einer Cloud, und einer beliebigen Anzahl Netzwerkteilnehmer, die über den zentralen Punkt kommunizieren. „Mit Zertifikaten oder VPN-Verbindungen wird wegen mangelnder Alternativen versucht, Datenströme zu schützen. Die Verwaltung einer eigenen Zertifikatskette ist allerdings mit enormem Aufwand verbunden. Zertifikate ohne diesen Verwaltungsaufwand sind unter Sicherheitsbetrachtungen wertlos. VPN-Verbindungen sind umständlich und können bei einer über einen zentralen Punkt hergestellten Verbindung zwischen zwei Netzwerkteilnehmern selbst bei korrekter Implementierung keine authentifizierte Ende-zu-Ende-Verschlüsselung herstellen. Der zentrale Firmenrechner oder die Cloud wird so automatisch zum integrierten Man-in-the-Middle, der jede Kommunikation belauschen und beliebig verändern kann. Gleichzeitig werden einem Innentäter, egal ob dieser bewusst oder unbewusst agiert, durch die fehlende Ende-zu-Ende Verschlüsselung Tür und Tor geöffnet“, erklärt Marius Schmidt, Gesellschafter und Leiter Entwicklung von SDT-Solutions, die Problemstellung, die zur Entwicklung der Software-Lösung AuthCryptor geführt hat.

Patentiertes „AuthCryptor“-Verfahren lässt Hacker auch in verteilten Systemen abblitzen

Das von SDT-Solutions entwickelte Verfahren ist vom Europäischen Patentamt patentiert und folgt den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem National Institute of Standards and Technology (NIST). AuthCryptor PP (PP für „Point to Point“) bietet höchsten Passwortschutz, weil keine Speicherung oder Übertragung von Passwörtern oder passwortäquivalenten Daten stattfindet. AuthCryptor NE (NE für „Network Edition“) ist eine weiterentwickelte Ende-zu-Ende-Verschlüsselung, die Verbindungen in Netzwerken mithilfe eines Vermittlers sichert. Zum Einsatz kommen ausschließlich bekannte und bewährte kryptografische Methoden. Das Funktionsprinzip beruht auf mathematischen Berechnungen, die von Client und Server für jede Authentifizierung durchgeführt werden. Das System akzeptiert nur passende Gegenstücke und deren Kombination. Unbefugte Dritte können zu keinem Zeitpunkt Daten abgreifen. Selbst ein gekaperter Sitzungsschlüssel gibt keine Hinweise auf vergangene oder zukünftige Schlüssel. „Die Beseitigung der bekannten Probleme im Bereich der Cybersicherung bei gleichzeitig einfacher Handhabung macht AuthCryptor NE zum zuverlässigen Torwächter für Netzwerkinfrastrukturen. Unser Verfahren ist auf dem Markt einzigartig“, erläutert Mathematiker Marcellus Schmidt, Gesellschafter von SDT-Solutions. „Wir verwenden elliptische Kurven. Das hat zur Folge, dass Schlüssel von nur 250 Bit Länge eingesetzt werden, wie vom BSI empfohlen. Bei anderen Verfahren schreibt das BSI für das gleiche Sicherheitsniveau Schlüssellängen von mindestens 2.000 Bit vor.“

Einfach zu implementieren und benutzerfreundlich

Die AuthCryptor-Produkte sind einfach zu implementieren und in bestehende Systeme nachrüstbar. Bei AuthCryptor NE muss lediglich ein Vermittler an einem Punkt der Netzwerkinfrastruktur installiert, die verfügbaren Dienste konfiguriert und die Netzwerkteilnehmer einmalig registriert werden. Der Vermittler dient ausschließlich als Verwaltungsstelle – die Netzwerkteilnehmer kommunizieren unabhängig vom Vermittler. Es entsteht kein zentrales Angriffsziel. Beliebig viele Netzwerkteilnehmer können eine authentifizierte und Ende-zu-Ende verschlüsselte Verbindung zueinander aufbauen, die selbst der zu AuthCryptor NE gehörende

Vermittler nicht belauschen kann. Durch die Benutzung von AuthCryptor NE werden Insider- und Man-in-the-Middle-Angriffe aller Art erkannt und abgewehrt. AuthCryptor NE agiert unabhängig von Dritten. Es werden keine digitalen Zertifikate einer PKI (Public-Key-Infrastruktur) benötigt. Selbst in unsicheren Netzen, wie dem Internet oder einem offenen WLAN, gewährleistet AuthCryptor NE die Integrität, Herkunft und Vertraulichkeit der Daten. Die Verwaltung kann von zentraler Stelle erfolgen und die Komplexität wächst auch nicht mit der Größe des Netzwerks. Das Hinzufügen oder Löschen eines Netzwerkteilnehmers ist mit konstantem Zeitaufwand durchführbar. Die Beseitigung der bekannten Probleme im Bereich der Cybersicherung bei gleichzeitig einfacher Handhabung macht AuthCryptor NE zum zuverlässigen Torwächter für Netzwerkinfrastrukturen.

[6.543 Zeichen]

Bildmaterial

[Image_AuthCryptor.jpg]

AuthCryptor ist eine Softwarelösung der SDT-Solutions GmbH für absolute Vertraulichkeit und Integrität für Daten in der Ende-zu-Ende-Verschlüsselung. Sie gewährleistet höchsten Schutz für Passwort und Daten auf Kommunikations- und Übertragungswegen. Das patentierte Verfahren basiert auf elliptischen Kurven und fun-

giert als Torwächter. Einfallstore in Kommunikations- und Übertragungswege werden konsequent geschlossen. Unternehmen jeder Größenordnung, Banken, Ärzte, Rechtsanwälte aber auch Privatpersonen beim Homebanking oder im Smart Home profitieren von dieser neuen Qualitätsstufe der Cybersicherheit. (Quelle SDT-Solutions)

Über SDT-Solutions

Die SDT-Solutions GmbH ist Spezialist für Datensicherheit, speziell Authentifizierungs- und Verschlüsselungsverfahren. Das 2016 gegründete Unternehmen hat seinen Hauptsitz im südbadischen Kappelrodeck. Das Team aus Informatikern und Mathematikern betreut seine Partner und Endkunden bei Software-Implementierungen und bietet Support in der DACH-Region. AuthCryptor, die Softwarelösung für absolute Vertraulichkeit und Integrität für Daten in der Ende-zu-Ende-Verschlüsselung, wurde im eigenen Haus entwickelt und das Verfahren ist vom Europäischen Patentamt patentiert.

Kontakt

SDT-Solutions GmbH
Erb 10, 77876 Kappelrodeck
Tel.: +49 (0)7842 98856
info@sdt-solutions.de
www.sdt-solutions.de