SecurITy made in Germany

sayTEC

Wie funktioniert sayTRUST?

Sichere Kommunikation und sicherer Zugang zu Daten und Anwendungen

VERSION 1.1
2019/06

Common Criteria EAL 4+
(im Zertifizierungsprozess)

2018 STEVIE GOLD WINNER GERMAN STEVIE AWARDS

SOFTSHELL VENDOR REPORT 2018 SOFTSHELL

2018|2019 INNOVATIV DURCH FORSCHUNG Ausgezeichnet durch den Softwerverband IBI5684REG

qualityaustria SYSTEMZERTIFIZIERT ISO 9001:2015 NR.21628/22

VPSC statt VPN – wir haben weitergedacht:

- Kommunikation innerhalb der Applikationsebene anstatt Netzwerk-Netzwerk-Kopplung
- Achtstufige Sicherheit - Schutz bereits vor dem Tunnel anstatt am Ende
- Eigene fälschungssichere und geschützt Zertifikate
- Komplett abgesicherte Arbeitsumgebung

Sicherheit muss einfach sein. Nach diesem Grundsatz wurde die Bedienoberfläche für sayTRUST Secure Access entworfen. Während bei herkömmlichen VPN-Lösungen immer ein Kompromiss eingegangen wird, hat sich die sayTEC AG bei der Entwicklung von sayTRUST Secure Access der von Kunden herangetragenen Anforderungen angenommen. Herausgekommen ist ein Werkzeug, das hohe Sicherheit und einfache Bedienung miteinander vereint.

Bei den Sicherheitsmerkmalen wurden neben allgemein anerkannten Standards (SSL, TLS, X.509 Zertifikat mit 2048-Bit, Diffie-Hellman Perfect Forward Secrecy in Abhängigkeit der persönlichen Anwenderzertifikats) weitere „Alleinstellungsmerkmale“ implementiert. Dazu gehört eine applikationsbasierte Verbindung im Tunnel (statt des üblichen Layer 2 oder Layer 3 VPN). So wird Schadsoftware bereits am Eingang des Tunnels erkannt und abgewehrt. Mit der eigenen CA (Certificate Authority) werden die Zertifikate selbst erstellt und nicht über eine fremde Stelle bezogen. Die gesamte Kommunikation wird aus dem Arbeitsspeicher (RAM) des Client-Rechners aufgebaut. So verbleiben auf dem Rechner und auf der Verbindungsstrecke keine Datenreste, die später eine Auswertung erlauben.

Damit ist auch die bei Hackern beliebte „Man in the Middle Attacke“ unmöglich. Für die verschlüsselte Kommunikation ist keine eigene virtuelle Netzwerkkarte und damit auch keine separate IP-Adresse aus dem zu schützenden Netzwerk erforderlich. Von außen sind das Netzwerk und dazugehörige Informationen unsichtbar. Auf dem Client-PC ist die Verbindung ebenfalls unsichtbar. Das Gerät hat und kennt keine Netzwerkinformationen vom zu schützenden Remote-Netzwerk.

Für den Anwender besonders angenehm ist, dass er seine Arbeitsumgebung in Form des sayTRUST Secure Access Sticks immer bei sich tragen kann. Der Administrator konfiguriert zentral die Berechtigung und damit die Arbeitsumgebung des Nutzers, sowie den Zugriff auf die Applikationen und Verzeichnisse. Einmal anmelden und der automatische Zugriff auf alle genehmigten Anwendungen ist gewährleistet - ohne lästige wiederholte Eingabe von Passwörtern – das wünschen sich Anwender. Der Passwort-

manager für Single-Sign-On sorgt für höchste Sicherheit. Dabei werden über die verschlüsselte Datenbank des Anwenders die Anmeldungen auf verschiedenste Anwendungen und/oder Plattformen mit den jeweiligen Passwörtern durchgeführt. Bei Aufruf einer beliebigen Anwendung kümmert sich das Single-Sign-On Modul im Hintergrund um die sichere Authentifizierung. Die einzelnen Anwendungen bleiben natürlich weiterhin mit unterschiedlichen Passwörtern geschützt.

Zielgruppen für mobile Anwendungen sind z.B. Außendienstmitarbeiter, Heimarbeitsplätze, Wartungstechniker von Dienstleistern oder Gruppen, die strikt nach Anwendungen getrennt sein müssen. In Schulen wird damit die Trennung in ein Schüler-, Lehrer- und Verwaltungsnetz gewährleistet. Im Krankenhaus werden die Patientenakten nur für berechtigte Personen aus dem medizinischen Bereich und der Verwaltung zugänglich gemacht. In der Industrie werden Daten und Zugänge für die Entwicklerteams sicher voneinander getrennt.