05 | 24

Automatisierung mit Ansible-as-Code

Sicherheit für eingehende E-Mails

Microsoft Teams als TK-Anlage

ISSN 1614-2888
€ 14,80
Österreich € 17,00
Luxemburg € 17,00
Schweiz CHF 24,00

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Zero Trust

Unter Verdacht

Moderne Strategien gegen bösartige Akteure

Richtlinien für das Active Directory

Domaincontroller schützen

Vertrauenszirkel

Zero Trust mit XplicitTrust

Die Zeit wird knapp

NIS-2-Richtlinie umsetzen

Sicherer Datenaustausch

Pointsharp Cryptshare 6.1

www.it-administrator.de

4 196583 214807 05

sayTEC sayTRUST VPSC

Sicher durchschleusen

von Thomas Bär

Mit VPNs stellen Administratoren den Zugriff für mobile User zur Verfügung. Jedoch ist es nicht immer gewollt, dass die Endgeräte auch zum Teil des Netzwerks werden. Zudem bringen klassische VPNs nach wie vor eine Reihe von Unzulänglichkeiten mit sich, etwa in der Verwaltung oder bei der Performance. Mit sayTECs sayTRUST VPSC steht ein anderer Weg des geschützten Zugangs offen, der im Test überzeugte.

Der Zugriff auf Applikationen und Daten ist für mobile Anwender beziehungsweise im Home Office der typische Anwendungsfall, den Administratoren bereitstellen. Es versteht sich dabei von selbst, dass dieser Zugriff für den Benutzer möglichst einfach sein soll. Die meisten Firmen setzen dafür auf ein klassisches VPN, das über das fremdverwaltete WLAN wie etwa eine Fritzbox eine Verbindung in das Firmennetzwerk aufbaut. Der Anwender setzt in seiner heimischen Netzwerkumgebung einen Laptop ein. Administratoren wie Benutzer beklagen bei der täglichen Arbeit mit solchen VPN-Programmen aber häufig eine ganze Reihe von Problemen: Software, die sich auf den Clientsystemen nur schlecht oder überhaupt nicht integriert, umständliche, proprietäre Hardware, die bei manchen Anwendungen zusätzlich benötigt wird, oder auch quälend langsame Verbindungen sind nur einige davon.

Das in Deutschland ansässige Unternehmen sayTEC stellt mit "sayTRUST VPSC – ZeroTrust Client Access" ein Werkzeug bereit, das diese Probleme nicht aufweist. Insbesondere relativiert das Produkt die größte Sicherheitslücke: die gespeicherten Zugangsdaten auf dem Endgerät. Kommt der heimische PC oder das private Laptop für Zugriffe zum Einsatz, gilt es, im Idealfall die Verbindung vom Heimrechner und dem Organisationsnetzwerk zu entkoppeln und zu isolieren. Es darf keinerlei Wechselwirkung zwischen den Netzwerken entstehen können, um etwaige Man-in-the-Middle-Attacken oder Manipulationen zu unterbinden.

Ein neuer Ansatz für VPNs

Bevor wir sayTRUST aus der Sicht des Users betrachten, wollen wir das dahinterliegende System beschreiben. Grundsätzlich besteht dieses aus einem Server und einer Clientkomponente, die typischerweise in Form eines USB-Access-Sticks daherkommt. Der Server kann als Hardware-Appliance oder als klassische Installation zum Einsatz kommen. Erwartungsgemäß gibt es verschiedene Ausbaustufen bei den Servern, die, je nach erforderlicher Anzahl gleichzeitiger Verbindungen, in den Varianten Basic, Professional und Enterprise zur Verfügung stehen. Optional bietet sayTEC auch eine HA-Appliance mit Schutz vor Hardwareausfall.

Auf der Clientseite stehen USB-Sticks mit Zweifaktor-(2FA) oder Dreifaktor-Authentifizierung (3FA) zur Auswahl. Der Anwender nutzt den USB-Stick, um die Zugriffssoftware für das VPSC (Virtual Protected Secure Communication) in den Clientspeicher zu laden. Das Programm startet und baut über das Internet eine Verbindung zum SayTRUST-Server im Netz auf. Dieser regelt den Zugriff auf erforderliche Ressourcen. Alternativ ließe sich die Software auch direkt auf dem Endgerät installieren, wobei jedoch die Sicherheit konzeptionell bedingt sinkt.

Im Gegensatz zu VPN-Technologien, so der Hersteller, setzen die Sicherheitsmechanismen bereits vor dem eigentlichen Kommunikationstunnel ein. Dies geschieht durch den koordinierten Einsatz mehrerer ineinandergreifender Sicherheitsstufen. So sind Daten und Netzwerk in einem höheren Grad geschützt als bei einer direkten LAN-LAN-Kopplung. Das Abwehrsystem ist dabei vielschichtig und in drei sogenannte Sicherheitsblöcke aufgeteilt. Nur wenn sämtliche ineinandergreifenden und voneinander abhängigen-

Sicherheitsstufen durchlaufen sind, baut das System die Kommunikation auf.

Im Sicherheitsblock 1 befindet sich die eindeutige persönliche Identifizierung des Anwenders, die aus biometrischen Informationen, einer PIN, einem Anwenderzertifikat mit 2048 Bit Länge und einer Verschlüsselung des Storage für den Zugriff auf die Verbindungsapplikation nach AES 256 Bit besteht. Der Sicherheitsblock 2 enthält die Verbindungssicherheit durch "Defense in Depth", bestehend aus dem einem VPSC-Tunneling direkt aus dem Client-Prozessspeicher, einer Diffie-Hellman-Kommunikationsverschlüsselung im Client-RAM und sogenannten APP-Socket-Verlängerungen im Client-RAM. Der dritte Sicherheitsblock betrifft die Netzwerkzugangskontrolle durch den sayTRUST-Server selbst. Das 2048-Bit-Anwenderzertifikat des VPSC-Kommunikationsclients, das durch die sayTEC-eigene CA signiert und überprüft wurde, ermöglicht Zugriffe auf lokale, mobile oder entfernte Anwendungen.

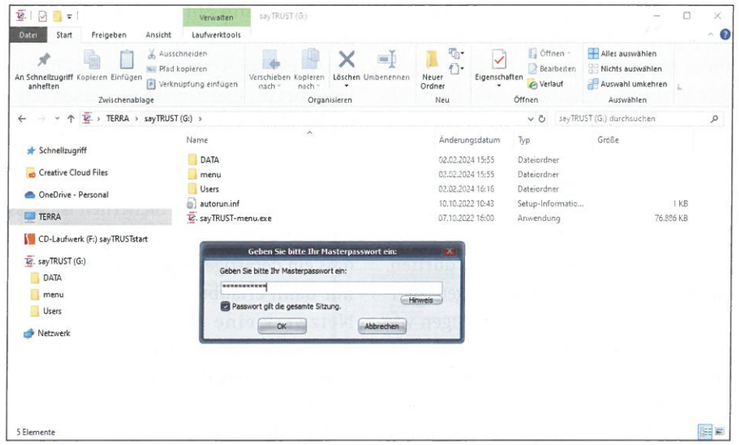

Bild 1: Ohne die Eingabe eines Passworts öffnet sich bei sayTRUST nicht einmal das Menü.

Keine Installation nötig, einfach USB-Sticks verteilen

Für einen Produkttest stellte uns der Hersteller den Zugriff auf eine Testumgebung mit vorkonfigurierter Umgebung zur Verfügung. Als Clientkomponente nutzten wir einen "sayTRUST ASB Access Client 3 Faktor" mit 16 GByte Speicher mit einem 32-Bit-Mikrocontroller und AES-256-AT32UC3A3256S-Verschlüsselung. Dabei lässt sich dieser so konfigurieren, dass ein Computer, in dem ein solcher USB-Client eingesteckt wird, diesen erst nach der biometrischen Identifikation überhaupt als Gerät erkennt. Im Einsatz werden IT-Profis ihren Benutzern vorkonfigurierte USB-Sticks an die Hand geben, mit denen diese dann direkt den Tunnel zum Unternehmensserver aufbauen. Die biometrische Erkennung erfolgte in unserem Fall per Identifikation des Fingerabdrucks. Der Endanwender muss unbedingt wissen, dass zunächst das Training für den Fingerabdruck ansteht, ehe der USB-Stick als Device im Windows-Explorer sichtbar ist und von dort aus die Verbindungssoftware startet. In unserem Fall reichte die begleitende Dokumentation, die das Verhalten der Leuchtdioden beim Einlernen erklärte.

Kinderleichte Sicherheit für den Anwender

Wir haben den USB-Stick mit PCs und Laptops unter Windows 10 und 11 getestet, die eine aktive Verbindung zum Internet besaßen, was eine Voraussetzung für den Einsatz ist. Auf dem uns zur Verfügung gestellten USB-Stick war das zum Verbindungsaufbau benötigte Zertifikat bereits installiert. Dies kann ein Administrator seinen Anwendern aber auch auf anderen Wegen etwa per Download oder via E-Mail übergeben. Ist ein Zertifikat erst einmal importiert und nutzbar, kann der Benutzer das sayTEC-Trust-Menü verwenden. Dieses ist insgesamt übersichtlich und gliedert sich in verschiedene Funktionsbereiche wie Verbinden, Remote Apps, Published Apps, Desktop, Portable Apps, Shares oder direkte Programmaufrufe. Was wie angezeigt wird, legt der Administrator fest.

Wir konnten in unserem Test jedoch nicht übersehen, dass das Design der Software etwas antiquiert wirkt. Während beispielsweise die Webseite die Grundfunktionalität ganz modern als Comic-Style-Video in einer Endlosschleife visualisiert und dem Zeitgeist entspricht, sind das Menü, das Layout und die Icons in der Software im Stil der frühen 2010er-Jahre geblieben. Das sind jedoch nur Hinweise im Sinne der B-Note, denn das hat auf die Funktionalität beim Benutzer keinen Einfluss.

Der wichtigste Klick hier ist der Menüpunkt "Verbinden", der eine Aufforderung

sayTEC sayTRUST VPSC

Produkt
Software für den verschlüsselten, internen und externen Zugang zu Unternehmensnetzwerken.

Hersteller
sayTEC
www.saytec.eu

Preis
Der kleinste Anwendungsfall umfasst eine Appliance (entweder als virtuelle Maschine, Installation oder als Hardware-System) mit fünf Zugriffslizenzen für Clients. Client-Zugriffslizenzen sind in Pakete zu 5, 25, 250 oder 500 verfügbar. Die USB-Token für den gesicherten Zugriff sind per se optional und auch ein Mischbetrieb ist möglich. In der kleinsten Softwarevariante beginnt der Preis bei rund 1655 Euro, die kleinste Appliance kostet zirka 2725 Euro. Fünf Zugriffslizenzen (clientbasiert) kosten 196,35 Euro, 250 sind für 8568 Euro zu haben. Ein biometrischer USB-Stick mit 16 GByte Speicherplatz kommt auf rund 345 Euro, es ist allerdings jeder USB-Stick einsetzbar.

Systemvoraussetzungen
Bei lokaler Installation ein beliebiger aktueller x64-Server mit klassischen Leistungsdaten für den Linux-Betrieb. Eine stabile Internetanbindung ist für die Appliance und die Clientcomputer zwingend erforderlich. Hinsichtlich des Clientrechners macht der Hersteller keine besonderen Angaben, daher ist von einer Kompatibilität mit allen aktuellen Windows-Versionen auszugehen.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

zur Eingabe einer PIN auf den Bildschirm beförderte. Diese vergibt der Administrator zuvor, danach erfolgte relativ zügig der Verbindungsaufbau und dadurch konnten wir nun auch auf die zuvor nicht aktiven Bereiche des Menüs zugreifen. Dies lief völlig logisch und leicht durchschaubar ab, sodass auch weniger erfahrene Anwender mit dem Einsatz dieses Clients kaum Probleme haben dürften. Im Bereich "Remote-Anwendungen" standen vorkonfiguriert Anwendungen wie Microsoft Word oder Excel bereit, die sich mittels Doppelklicks starten und verwenden ließen. Beim erstmaligen Klick auf eine Applikation innerhalb einer solchen Sitzung muss der User sich allerdings noch einmal mittels Benutzernamen und Passwort authentifizieren, bevor er Zugriff auf die vorkonfigurierten Remote- oder auch Webanwendungen erhält. Letztendlich handelt es sich um publizierte Remote-Apps im Rechenzentrum, auf die nun ein getunnelter Zugriff erfolgt.

Möchte der Nutzer dann beispielsweise die erstellten Dokumente abspeichern, kann dies problemlos sowohl auf dem USB-Stick (vorausgesetzt die Dateien sind nicht zu groß) oder auch auf lokalen Ressourcen wie den Laufwerken des Client-PCs erfolgen. Diese können, sofern vom Administrator über die Remote-Desktop-Konfiguration zugelassen, mittels der bekannten Laufwerksbuchstaben in die Sitzung eingebunden werden. Gibt der Anwender hierbei keinen Buchstaben an, wählt die Software den nächsten freien oder einen fix vorgegeben aus. Dies kann entweder als durchgereichte Anmeldung via LDAP oder durch den eingetragenen Nutzer mit einem Passwort für den Zugriff geschehen. Dabei handelt es sich dann um UNC-Freigaben, die der Client lokal initiiert.

Sehr gut aus Sicht der Sicherheit ist, dass der Administrator zuvor festlegen kann, dass ein derartiger Zugriff beispielsweise nur dann erlaubt ist, wenn das fremde Netzwerk eine Adresse in der Form "192.168.x.y" besitzt. Eine grundsätzliche Unterscheidung der Umgebung wäre somit denkbar, setzt aber organisatorische Rahmenbedingungen voraus, dass beispielsweise das Heimnetzwerk für den Home-Office-Arbeitsplatz einen bestimmten IP-Adressbereich hat. Deutlich sinnvoller und entsprechend der Philosophie, dass nichts auf dem eigentlichen Client-PC zurückbleibt, ist das Prozedere, dass der Benutzer seine Dateien im Dateisystem des dahinterliegenden Remote-Desktop-Servers speichert.

Bild 2: Ein biometrisch geschützter USB-Stick mit der sayTRUST Software an Bord ist der Zugangsschlüssel zu entfernten Ressourcen.

Blickdichte Verbindungen

Administratoren erwarten in der Regel, dass eine derartige Software eine virtuelle Netzwerkkarte auf dem Clientsystem einrichtet, um auf diese Weise den Tunnel über das Internet aufzubauen und sicher zu betreiben. Die Firma sayTEC verwendet hier, wie bereits eingangs benannt, ein anderes Konzept: Virtual Private Tunneling (VPT). Die Verbindung wird dabei auf der Anwendungsebene aufgebaut. Auf diese Weise ist keine direkte Koppelung über das Netzwerk erforderlich.

Daher galt unser erster Blick auf den Clientsystemen nach dem Aufbau der Verbindung zum sayTRUST-Server auch den Netzwerkeinstellungen und danach der Prozessliste auf dem System. Eine zusätzliche Netzwerkkarte war unter Windows nicht zu entdecken und zudem konnten wir verifizieren, dass es keine mit einem Sniffer identifizierbaren direkten Datenpakete gibt, aus denen ein unerwünscht mitprotokollierender Angreifer sinnvolle Informationen abgreifen könnte.

Die Fachleute von sayTEC erläuterten uns, dass die Verbindung auf Prozessebene im User-Kontext des jeweiligen Programms entsteht. Das System verlängert dabei quasi die TCP- und UDP-Sockets in das Firmennetzwerk. Der Vorgang erfasst nur die vom Administrator konfigurierten Anwendungen und dabei auch nur die für diese konfigurierten Zieladressen und Ports. Netzintern erscheinen diese Anwendungen mit den Adressen des sayTRUST-Servers. Dieser bestimmt dabei auch mithilfe von Listen, welche Programme ein Benutzer (oder auch eine Gruppe) über die Tunnel verwenden darf. Alle nicht freigegebenen Anwendungen sind von der Verbindung ausgeschlossen. Zusätzlich besitzen Systemverwalter auch noch die Möglichkeit, Clientanwendungen gezielt auszuschließen. Beendet der Nutzer die verschlüsselte Verbindung, bleiben keinerlei auswertbare Spuren auf seinem Computer zurück. Grundsätzlich eignet sich daher das von sayTEC angebotene System für die Verwendung in Rechnern, deren Sicherheitsstatus nicht von einem Administrator überprüft wird oder werden kann.

Backend lässt keine Wünsche offen

Das Gegenstück des Clients ist erwartungsgemäß die Serverumgebung. Im Rahmen unserer Tests hatten wir die Möglichkeit, uns in der Demoumgebung umzuschauen. Den Server beziehungsweise die Appliance verwaltet der Administrator in erster Linie über eine Webkonsole. Die lokale Konsole zeigt lediglich einen Dialog zum Anpassen der IP-Adresse – weitere Einrichtungsschritte sind hier nicht vorgesehen. Auch sonst zeigt sich das Basisbetriebssystem eher

verschlossen. Ein SSH-Zugriff auf die Linux-Konsole ist nur möglich, sofern der Administrator dies über das Webinterface explizit aktiviert. Laut sayTEC ist dies aber auch nur höchst selten notwendig.

Die Grundkonfiguration besteht in erster Linie aus dem Einbinden in die vorhandene Netzwerkumgebung und hat ein wenig was von der Einrichtung eines Routers. Rund 30 Minuten Zeit ist für die Basiskonfiguration vorzusehen, so der Hersteller. Der IT-Profi füllt dabei die klassischen Felder mit Informationen: IP-Adresse, Router-Gateway-Adresse, DNS-Einträge, Syslog-Server oder Proxy-Anbindung. Die Benutzerverwaltung in diesem Bereich der Webkonsole ist nicht für den Clientzugriff gedacht, sondern steuert die administrativen Aufgaben.

Welche Teilbereiche der Dialoge zur Verfügung stehen sollen, definiert der Systemverantwortliche mit einigen Mausklicks. Gilt es beispielsweise, ein Konto für einen Backup-Verantwortlichen anzulegen, sieht dieser auch nur die entsprechenden Dialoge, die für diese Rolle erforderlich sind. Auch an eine Sicherung wurde gedacht: Der Server verfügt über eingebaute Backup- und Restore-Funktionen. In einem unserer Tests war das Backup der Zertifikate und Einstellungen in wenigen Augenblicken erledigt. Eine zügige Sicherung, typischerweise vor einem Update oder größeren Konfigurationsänderungen, ist somit gar kein Problem.

Auch sonst findet der Admin einige äußert gut umgesetzte Ideen, wie den "Activate Panic Login". Hierbei handelt es sich um eine Möglichkeit, den aktuellen Stand einzufrieren und temporäre Zugriffszertifikate für den externen Zugriff zu aktivieren. Systemhäuser könnten sich so im Bedarfsnotfall und auf Wunsch des Kunden zügig auf das System aufschalten oder holen sich über diesen Weg eine Unterstützung vom Hersteller. In diesem Szenario kappt der Server jedoch alle zuvor aktiven Verbindungen. Ist die Ausnahmesituation wieder beendet, lässt sich die "Panic"-Funktionalität wieder deaktivieren und der reguläre Zugangsbetrieb ist wieder möglich. Je nach vom Administrator gewählter Einstellung versorgt sich

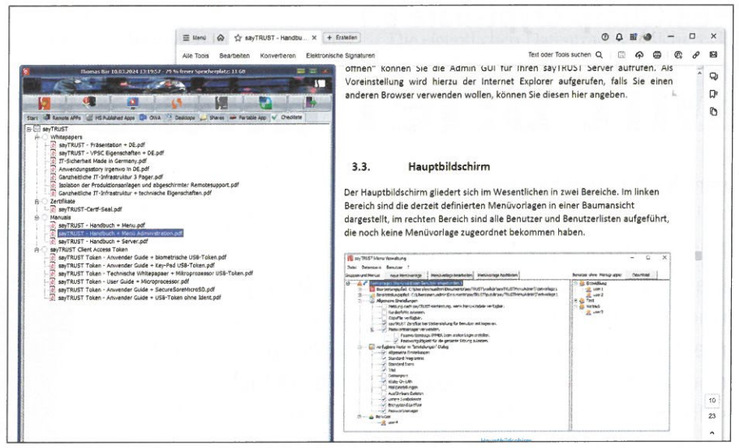

Bild 3: Der USB-Stick eignet sich auch zur Ablage von Dateien des Anwenders.

das System selbstständig mit Updates über das Internet, sofern der entsprechende Vertrag mit dem Anbieter besteht. Ansonsten installiert der IT-Verantwortliche Updatedateien manuell über einen entsprechenden Webdialog.

Die eigentliche Hauptarbeit verrichtet der Administrator jedoch im Menüabschnitt "Remote Access". Hier legt er für die verschiedenen Personen und Gruppen die passenden Zugriffe anhand von Policies an und kann diese auch verwalten. Dazu gehören Einstellungen wie die Richtlinie, ob der Nutzer bei der Anmeldung zwingend eine PIN angeben muss, wie komplex diese sein soll und ob sie geändert werden muss. Alle diese Änderungen und Einstellungen konnten wir im Test leicht vornehmen und unserem Client präsentieren. Bei den Nutzergruppen bietet die Software unter anderem auch die Möglichkeit, die Server mit einem bestehenden LDAP-Server zu verbinden. Zudem können Administratoren auch mit lokalen Gruppen arbeiten, über die beispielsweise ein zeitlich begrenzter Zugang für externe Consultants realisiert wird.

Grundsätzlich zeigte sich auch die Konfiguration des Servers selbsterklärend, genau so wie auch bei den Clients. Zwar erfordern die Servereinstellung verständlicherweise ein größeres IT-Know-how als die auf den Endanwender ausgerichteten Clients, aber insgesamt sollten sie einem erfahrenen IT-Profi keine Probleme bereiten.

Fazit

In unseren Tests hat uns sayTRUST sehr gut gefallen. Das komplette Loslösen von Konfigurationsaufwänden auf dem eigentlichen Endgerät ist überaus charmant. In einer künftigen Version, so durften wir bereits erfahren, wird die Bereitstellung der USB-Sticks mit der Clientsoftware noch einmal dahingehend überarbeitet, dass ein Self-Service möglich ist, bei dem der Anwender beispielsweise am Firmen-PC seinen Stick für den mobilen Zugriff selbst füllt. Bis dahin gilt jedoch auch, dass jeder IT-Profi, der mobile Anwender betreuen muss, es zu schätzen weiß, dass er exakt vorkonfigurierte USB-Sticks an seine Anwender rausgeben kann. Diese setzen den Stick dann einfach und sicher an beliebigen Endgeräten ein. Durch die Regelung mittels Policies ist der IT-Verantwortliche sehr gut in der Lage, die meisten Anwendungs- und Einsatzfälle im Vorfeld einzurichten *(jp)*

So urteilt IT-Administrator

Benutzeradministration	6
Verbindungsverwaltung	7
Sicherheit	9
Clientunabhängigkeit	9
Benutzerfreundlichkeit	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik