Sicherheit beginnt mit der Identitätsprüfung des Nutzers und der Autorisierung vor einem PC

Post Zero Trust

WhitepapersayTRUST UZE – Universal Zero Trust Exchange

sayTEC AG

sayTRUST UZE Technisches Whitepaper

Universal Zero Trust Exchange Architektur und die technische Funktionsweise

sayTRUST UZE setzt die Sicherheitsentscheidung vor die Freigabe einer Anwendungsbeziehung. Die Plattform verbindet persönliche Identität, einen gebundenen UZE-Client, geschützte Sitzungsverarbeitung und serverseitige Regeln miteinander. Der Benutzer arbeitet mit freigegebenen Anwendungen, ohne einen allgemeinen Zugang zum geschützten Netz zu erhalten.

Die Sicherheitskette beginnt bei der eindeutigen Identifikation und Autorisierung des Benutzers vor dem Rechner. Erst danach werden die geschützte Client-Umgebung aktiviert, Richtlinien und Sicherheitszustand geprüft und die konkret freigegebene Kommunikation aufgebaut.

Vergleich Architekturen VPN, Zero-Trust und Post-Zero-Trust

Klassische VPN-Lösungen koppeln einen entfernten Rechner trotz Verschlüsselung technisch an ein Netzwerk oder einen Netzbereich. Wird der Client kompromittiert, kann diese Verbindung selbst zum Angriffsweg werden.

Zero-Trust und ZTNA verbessern die Kontrolle. Klassisches Zero Trust folgt „never trust, always verify“, gewährt nach erfolgreicher Prüfung aber weiterhin Zugriff auf definierte Ressourcen bzw. Netzwerkbereiche. Damit bleibt eine erreichbare Angriffsfläche bestehen. Werden Benutzerkonto, Token, Session oder Endgerät erfolgreich übernommen, kann ein Angreifer innerhalb der erteilten Berechtigungen wie ein legitimer Nutzer auftreten. MFA und kontinuierliche Prüfung reduzieren dieses Risiko, eliminieren es aber nicht.

Post-Zero-Trust führt den Gedanken weiter: Nicht das Netzwerk wird geöffnet, sondern nur die autorisierte Beziehung zu einer Anwendung. Autorisierte Kommunikationsbeziehung wird isoliert und verlagert die Sicherheitsentscheidung konsequent vor den Kommunikationsaufbau.

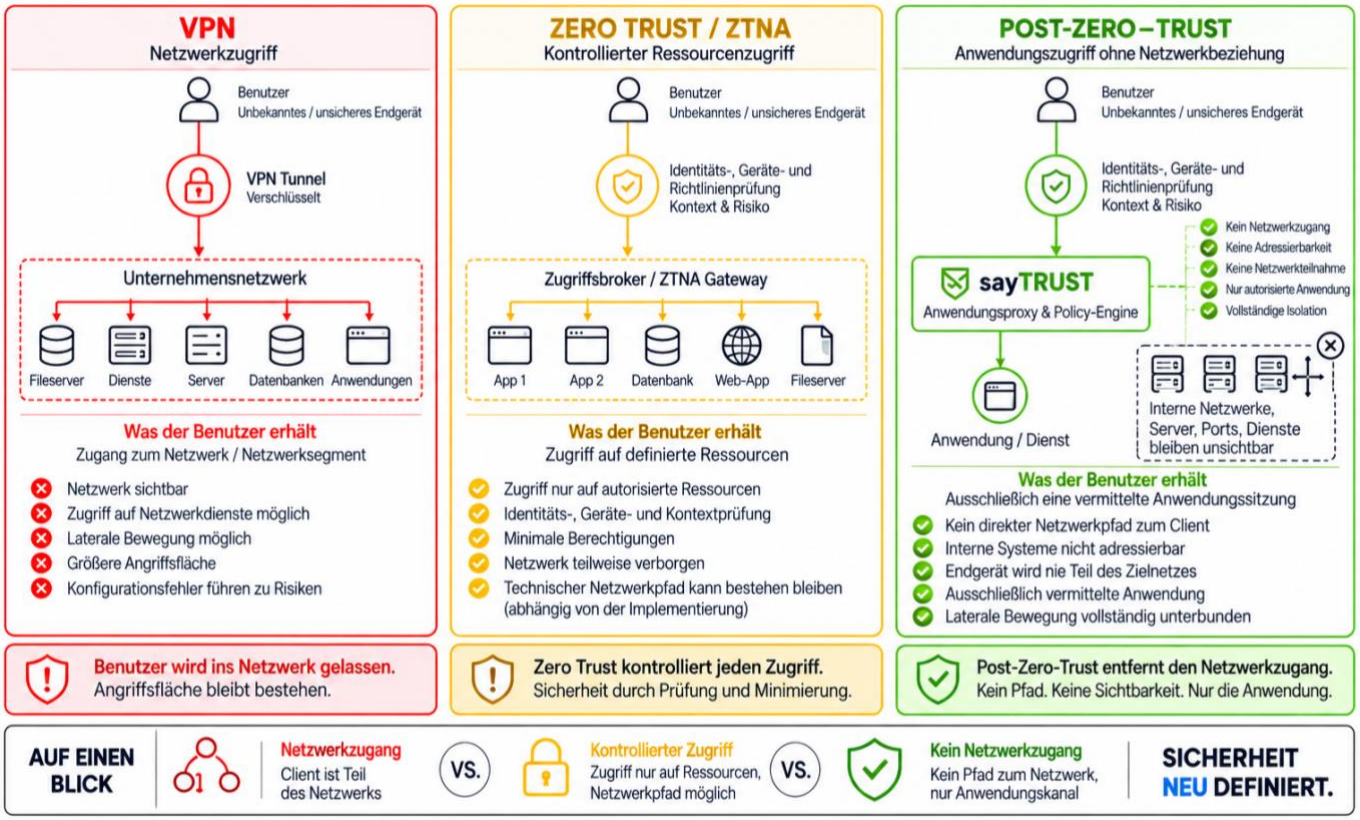

Abb. 1: VPN, Zero Trust und Post Zero Trust im direkten Architekturvergleich.

Der Arbeitsplatzrechner ist einer der kritischsten Punkte einer Zugriffsarchitektur. Er befindet sich außerhalb der unmittelbaren Kontrolle des Rechenzentrums und kann gleichzeitig zum Ausgangspunkt für unerwünschte Kommunikationswege werden. sayTRUST UZE betrachtet den Client deshalb nicht nur als Transportmittel für einen Tunnel, sondern als kontrollierten Bestandteil der Sicherheitsarchitektur.

Die Verbindung aus Benutzeridentifikation, kontrollierter UZE-Client-Aktivierung, geschütztem temporärem Arbeitsspeicherkontext, zentralem UZE-Server und vorgelagerten Prüfungen reduziert die Abhängigkeit von einem einzelnen Kontrollpunkt am Gateway. Die Sicherheitslogik erstreckt sich vom Menschen vor dem Rechner bis zur konkret autorisierten Beziehung.

Post-Zero-Trust isoliert von Identität bis Anwendung und lässt nur autorisierte Kommunikationsbeziehung zu.

Abb. 2: Fünf Schritte vom identifizierten Benutzer zur autorisierten Anwendung.

1. Architektur und Schutzbereiche

Die Kommunikationsstrecke beginnt beim User und seinem Gerät. Sie verläuft durch ein möglicherweise fremdes Netz und den Transportweg bis zur UZE-Serverumgebung und der Zielanwendung. UZE behandelt jeden dieser Abschnitte als eigene Sicherheitsaufgabe: Identität vor der Client-Token-Aktivierung, geschützte Kommunikation über den gesamten Transportweg, Policy-Prüfung am Server und begrenzte Freigabe am Ziel.

Der UZE-Client ist entweder ein persönlicher Hardware-Client oder eine gerätegebundene Softwareinstallation. Der UZE-Server verwaltet die Identitäten, Zertifikate, Regeln und freigegebenen Beziehungen. Der Client erhält kein allgemeines internes Routing; die freigegebene Beziehung führt zu der definierten Anwendung beziehungsweise bei UZE Plus zu ausdrücklich konfigurierten Systemen.

Abb. 3: Identität, geschützte Sitzung und Zielkontrolle greifen ineinander.

2. Benutzeranlage Zertifikat und Policy

2.1 Verzeichnisanbindung und manuelle Benutzer

User können auf zwei parallel nutzbaren Wegen angelegt werden. Erstens importiert die Administration Gruppen und Benutzer aus LDAP. Sie weist ihnen Regeln für Anwendungen, Zugriffe und, soweit für eine dedizierte Beziehung vorgesehen, Netzsegmente zu. Regeln erlauben, blockieren oder isolieren die jeweilige Kommunikation. Zweitens können Benutzer unabhängig vom LDAP manuell angelegt werden, etwa externe Zulieferer oder Personen außerhalb des Unternehmensverzeichnisses. Auch diese Benutzer erhalten eigene Zertifikate und auf ihren Zweck begrenzte Policies.

2.2 Integrierte Zertifizierungsstelle und Enrollment

Mit dem UZE-Server wird eine eigene Certificate Authority installiert. Sie erstellt benutzerbezogene Zertifikate. Die Ausgabe kann administrativ oder über das integrierte Enrollment mit Vorlagen für Benutzer und Clientvarianten erfolgen. Beim ersten Start wird das verschlüsselte Zertifikat an den konkreten Kommunikationsclient gebunden. Die Bindung berücksichtigt Geräte- beziehungsweise Token Merkmale einschließlich Hardwarekennung; eine kopierte Installation ist damit nicht ohne erneute Zuordnung auf einem anderen Gerät nutzbar. Wird sie auf einem anderen Ort genutzt, werden Original und kopierte Zertifikate gesperrt und können nicht mehr genutzt werden.

Bei einem Hardware-Client liegt das Benutzerzertifikat zusätzlich im verschlüsselten Tokenbereich. Bei der Softwarevariante wird es an die Installation auf dem definierten Rechner gebunden. Die CA und ihre Zertifikate werden im geschützten Serverbereich verwaltet; Administrationsrollen können die Zuständigkeiten für User, Policies und Zertifikate trennen.

2.3 Anwendungsregeln und Mischbetrieb

Die Administration definiert Anwendungen über Freigabe- und Sperrregeln. UZE unterstützt drei Ursprünge, die in einem persönlichen Menü kombiniert werden können: Anwendungen im geschützten Zielnetz oder auf Anwendungsservern, portable Anwendungen auf dem Token und lokal installierte Programme auf dem verwendeten Rechner. Regeln können einzelne Anwendungen zulassen, ihre Kommunikation isolieren oder Anwendungen und Verbindungen blockieren.

Ursprung	Technische Beziehung und Beispiel
Remote-Anwendung	Eine veröffentlichte Citrix- oder Terminalserver-Anwendung wird über die freigegebene UZE-Beziehung erreicht. Für die Nutzer müssen die üblichen eingehenden Anwendungsports nicht geöffnet werden.
Portable Anwendung	Telefonie, Videokonferenz oder ein portables Office-Programm kann vom geschützten Clientmedium gestartet und mit der zugewiesenen Beziehung verbunden werden.
Lokal installierte Anwendung	Ein Programm auf dem Rechner wird als Prozess freigegeben; die Policy ordnet ihm den zulässigen Dienst und das Ziel zu.

Die Formen lassen sich in einer Sitzung mischen. Beispielsweise kann ein Nutzer eine veröffentlichte Fachanwendung aus dem Rechenzentrum öffnen, ein portables Kommunikationsprogramm vom Token verwenden und zugleich eine lokal installierte Anwendung über UZE mit ihrem zugewiesenen Ziel verbinden. Auch lokale Anwendungen oder sonstige Netzkommunikation können für diese Sitzung gesperrt werden. Webanwendungen und veröffentlichte Dienste benötigen dabei keine allgemein nach außen freigegebenen Ports in das geschützte Netzwerk.

3. Aktivierung und Aufbau einer Sitzung

3.1 Persönlichen Client aktivieren

Bei der Hardwarevariante wird der Token erst nach der für ihn vorgesehenen Prüfung aktiviert, etwa über Biometrie oder PIN. Der UZE-Kommunikationsclient ist an diesen Token gebunden. Bei der Softwarevariante bindet die erste Ausführung den Client und das verschlüsselte Zertifikat an den installierten Rechner. Ein Hardware-Token kann dem berechtigten Nutzer an unterschiedlichen Rechnern dienen; eine Softwareinstallation ist dagegen an ihr Gerät gebunden.

Nach der Aktivierung öffnet sich das persönliche Anwendungsmenü. Für den Zugriff auf die integrierte Single-Sign-On-Datenbank gibt der User sein Datenbankpasswort ein. Die Datenbank verwendet die KeePass-Bibliothek und ist selbst verschlüsselt; bei der Hardwarevariante liegt sie im verschlüsselten Tokenbereich. Der Zertifikats-PIN für den Verbindungsaufbau kann vom User eingegeben oder aus dieser Datenbank bereitgestellt werden.

3.2 Zertifikat und weitere Faktoren prüfen

Vor der Anwendungsfreigabe prüft UZE das Benutzerzertifikat und die Zuordnung zum aktivierten Client. Eine veränderte oder kopierte Bindung wird nicht als gültiger Client akzeptiert. Hinzu kommen die für diesen Zugang vorgesehenen Faktoren, etwa persönliche Token Aktivierung, Zertifikats-PIN und OTP über einen externen Authenticator. Diese Schritte erfüllen unterschiedliche Aufgaben und greifen vor der Freigabe ineinander.

Fehlversuche bei der Zertifikats-PIN werden mit zunehmend längeren Wartezeiten beantwortet. Dadurch werden automatisierte Eingabeversuche gebremst. Die konkrete Sperr- und Entsperrregel gehört zur jeweiligen Serverkonfiguration.

3.3 Geschützte Kommunikation und PFS

Nach erfolgreicher Prüfung erzeugt die Sitzung temporäre kryptografische Schlüssel mit Perfect Forward Secrecy. Sitzungsbezogene Parameter werden im geschützten flüchtigen Arbeitsspeicher verarbeitet. Daten, die ein portables Programm technisch persistent ablegen muss, liegen im verschlüsselten Tokenbereich; auf lokalen Speichermedien des verwendeten Rechners werden durch den UZE-Prozess keine temporären Sitzungsdaten abgelegt.

Der UZE-Server prüft die Anwendungs-Policy und stellt nur die definierte Beziehung bereit. Prozess, Ziel und Dienst beziehungsweise Port bilden die technische Begrenzung für eine lokal installierte Anwendung. Der User sieht im Menü seine zugewiesenen Anwendungen, nicht frei adressierbare interne Server oder Segmente.

3.4 Sitzungsende und Unterbrechung

Mit dem Sitzungsende endet die Freigabe der Kommunikationsbeziehung; temporäre Sitzungsinformationen im flüchtigen Arbeitsspeicher werden entfernt. Temporäre Daten portabler Anwendungen im Token werden im regulären Ablauf gelöscht. Wird der Token vorher entfernt, bleiben eventuell vorhandene Daten im verschlüsselten Bereich und sind ohne persönliche Token Aktivierung nicht zugänglich.

Wird lediglich die Transportverbindung unterbrochen, baut der Client die zulässige Beziehung nach Wiederverbindung erneut auf. Der Nutzer kann anschließend mit den freigegebenen Anwendungen weiterarbeiten. UZE ist für den Zugriff aus internen, fremden und mobilen Netzen nach demselben Identitäts- und Policy Prinzip ausgelegt.

4. Bedienung und Bereitstellung

Der Ablauf am Arbeitsplatz ist bewusst einfach: Clientmedium anschließen oder gerätegebundenen Client starten, persönliche Prüfung durchführen, das eigene Menü öffnen und die freigegebene Anwendung wählen. Das Menü wird zentral bereitgestellt. Änderungen an Anwendungen und Zugangsregeln werden über die UZE-Verwaltung verteilt, sodass Nutzer auch an wechselnden Arbeitsplätzen die ihnen zugewiesene Arbeitsumgebung vorfinden.

Der Benutzer kann eine Fachanwendung im Rechenzentrum, ein portables Programm oder ein lokales Programm verwenden, ohne die darunterliegenden Zieladressen und Netze bedienen zu müssen. Dieses einheitliche Menü trennt die Bedienung von der technischen Platzierung der Anwendungen.

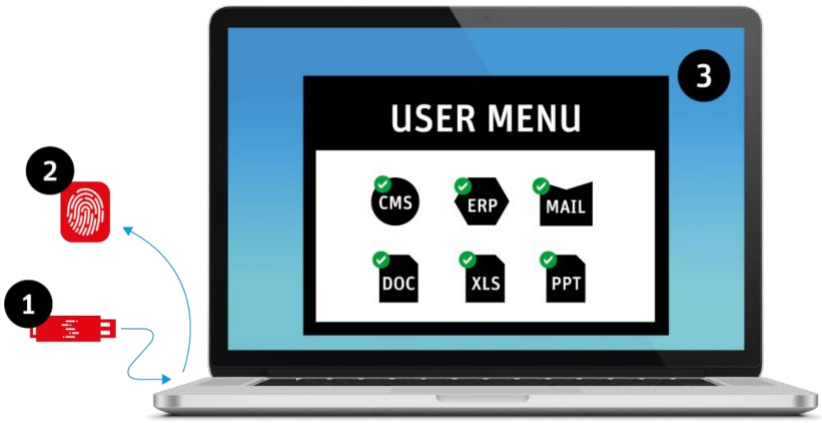

Abb. 4: Schematisches persönliches Anwendungsmenü aus der sayTEC Präsentation.

5. Clientvarianten und gerätebezogene Lizenzierung

Abb. 5: Der Client wird Teil der Sicherheitsarchitektur und nicht bloß Verbindungsmittel.

Die UZE-Clientvarianten teilen den Kommunikations- und Policy-Ansatz. Sie unterscheiden sich vor allem durch Aktivierungsverfahren und Hardwareaufbau. Flashbasierte verschlüsselte biometrische Varianten und

mikroprozessorbasierte Sicherheitstoken können in derselben Umgebung neben PIN- und Softwarevarianten betrieben werden. Der Token ist bei einer geschützten Variante vor persönlicher Aktivierung nicht als freigegebenes Clientmedium nutzbar.

Abb. 6: Beispiele der Hardwarevarianten aus der sayTEC Produktpreisliste. Die Softwarevariante ist gerätegebunden.

Clientvariante	Persönliche Aktivierung	Aufbau
Software-Client	Anmeldung und Zertifikats-PIN	An eine Installation auf einem definierten Rechner gebunden
Biometrie-Client	Biometrie oder Passwort	Verschlüsselter USB-Flash-Token
Mikroprozessor-Biometrie-Client	Biometrie auf dem Sicherheitstoken	Mikroprozessorbasierter USB-Token
USB-Client	Zertifikats-PIN	Portabler USB-Flash-Client
USB-PIN-Code-Client	Code und Zertifikats-PIN	Verschlüsselter USB-Client

Die Client-Zugriffslizenzierung ist gerätebezogen. Ein persönlicher Hardware-Token kann auf mehreren Rechnern verwendet werden. Eine Softwarelizenz ist an die jeweilige Clientinstallation gebunden; benötigt derselbe Nutzer mehrere Softwarearbeitsplätze, werden diese als separate Client-Devices lizenziert. Das Serverbetriebssystem enthält fünf Client-Zugriffslizenzen. Erweiterungspakete werden für 5, 25, 250 und 500 Client-Devices angeboten.

Auch im internen Netz kann der UZE-Zugang für Endgeräte eingesetzt werden, die keinen allgemeinen Zugriff auf das Infrastrukturnetz erhalten sollen. Externe Geräte und private Arbeitsplätze folgen demselben Prinzip: Die Identität und die freigegebene Anwendung entscheiden über die Beziehung, nicht der Standort des Rechners.

6. Servermodelle UZE Plus und Cluster

UZE wird als Serverbetriebssystem auf eigener Hardware oder einer unterstützten virtuellen Plattform sowie als physische Appliance bereitgestellt. Die Klassen Basic, Professional und Enterprise unterscheiden sich in der maximal vorgesehenen Anzahl gleichzeitiger UZE-Verbindungen. Die Anzahl der im Grundumfang enthaltenen Client-Zugriffslizenzen beträgt jeweils fünf; zusätzliche Geräte werden getrennt lizenziert.

Klasse	Maximale Verbindungen	Enthaltene Client-Zugriffslizenzen
Basic	25	5
Professional	250	5
Enterprise	Lizenzseitig unbegrenzt; Kapazität nach Plattformauslegung	5

6.1 Dedizierte Kommunikation mit UZE Plus

UZE Plus verbindet definierte Maschinen, Server und Standorte. Für jede Beziehung legt der Server fest, welche Gegenstellen miteinander kommunizieren und welche Dienste und Daten dafür freigegeben sind. Die gegenseitige Maschinenidentität und die serverseitigen Zielregeln verhindern, dass eine Standortanbindung

automatisch eine pauschale Freigabe aller Systeme bedeutet. Das Erweiterungsmodul beziehungsweise die UZE Plus Appliance unterstützt bis zu zwölf definierte Maschinen- oder Netzbeziehungen.

6.2 Aktiver Clusterbetrieb

Für Hochverfügbarkeit arbeiten mehrere UZE-Serverknoten aktiv im Cluster. Der Master-Cluster ist die zentrale Verwaltungsinstanz und verteilt Policies und Zertifikate an die anderen Knoten. Ein Load Balancer oder eine entsprechend konfigurierte Verteilung leitet neue Anfragen per Round Robin oder nach aktueller Last an verfügbare Server. Fällt ein Knoten aus, übernimmt ein anderer verfügbare Verbindungen beziehungsweise neue Sitzungen die Kommunikation. Die HA-Appliance übernimmt Lizenzumfang und Verbindungskapazität des zugeordneten Masters; Client-Zugriffslizenzen werden für den redundanten Knoten nicht erneut benötigt.

7. Protokollierung und Auswertung

UZE protokolliert unter anderem die Aktivierung des Clients, Zertifikats- und Faktorprüfungen, den Aufbau der freigegebenen Beziehung sowie deren Beendigung. Informationen zum verwendeten Clientrechner können beim Verbindungsaufbau aufgenommen werden. Der Client überträgt diese Informationen innerhalb der geschützten Kommunikation an den UZE-Server; er benötigt dafür keinen allgemeinen Zugang zum geschützten Netz.

Die Administration kann die internen Protokolle und Auswertungen der UZE-Plattform verwenden. Alternativ oder ergänzend werden Ereignisse an einen Syslog-Server übertragen, wo sie nach den Regeln des Kunden mit weiteren Daten korreliert und ausgewertet werden. Die Protokollierung dokumentiert die Sitzung; sie ist von der Identitäts- und Policyentscheidung vor der Freigabe zu unterscheiden.

Fazit

sayTRUST UZE verbindet persönliche Aktivierung, gebundene Zertifikate, geschützte Sitzungsverarbeitung und eine explizite Anwendungs-Policy zu einer durchgängigen Zugriffskette. Die gleiche Architektur unterstützt Anwendungen aus dem Rechenzentrum, portable Programme und lokal installierte Software. Hardware- und Software-Clients, UZE Plus und aktiv betriebene Servercluster erweitern diesen Ansatz auf unterschiedliche Arbeitsplätze, Maschinen und Standorte.