sayTEC

WHITEPAPER

Post Zero Trust und Cyberresilienz

Sicherheit beginnt mit der Identität - vor dem Rechner. Und Cyberresilienz endet erst mit gesicherter Wiederherstellungsfähigkeit.

- **Identität vor Zugriff**
- **Policy vor Kommunikation**
- **Anwendung vor Netzwerk**
- **Recovery als Fähigkeit**

Yakup Saygin
Vorstand Entwicklung & Technik | sayTEC AG

Stand: August 2026

Inhalt

1. Sicherheit beginnt mit der Identität
2. Die Sicherheitskette beginnt beim Menschen
3. Vom geschützten UZE-Client in eine temporäre Laufzeitumgebung
4. Sicherheit muss vor dem Tunnel beginnen
5. Zero Trust war ein Meilenstein – aber kein Endpunkt
6. VPN verbindet. Zero Trust kontrolliert. Post Zero Trust isoliert.
7. Nicht weniger Netzwerkzugang – sondern keinen allgemeinen Netzwerkzugang
8. Auch das Endgerät gehört zum Sicherheitsmodell
9. Zero Footprint: Sicherheit darf keine unnötigen Spuren hinterlassen
10. Kryptografie ist notwendig – aber noch keine Architektur
11. Sicherer Zugriff allein ist noch keine Cyberresilienz
12. Der „Tresor im Tresor“: mehrere Ebenen einer gemeinsamen Sicherheitsarchitektur
13. Backup ist eine Technologie – Recovery ist eine Fähigkeit
14. Resilienz muss getestet werden
15. Post Zero Trust und Cyberresilienz gehören zusammen
16. Weniger Angriffsfläche statt immer mehr Schutzschichten
17. Die praktische Umsetzung bei sayTEC
18. Der eigentliche Paradigmenwechsel
19. Fazit: Sicherheit beginnt mit der Identität

Executive Summary

Dieses Whitepaper zeigt, warum Zugriffssicherheit vor dem Tunnel beginnen muss und warum Cyberresilienz erst mit belastbarer Wiederherstellungsfähigkeit vollständig ist. Der Begriff „Post Zero Trust“ bezeichnet dabei das in diesem Whitepaper beschriebene sayTEC-Architekturmodell: Es ergänzt Zero Trust, ersetzt dessen Grundsätze jedoch nicht. Die praktische Umsetzung bei sayTEC erfolgt mit sayTRUST UZE – Universal Zero Trust Exchange.

1. Identität zuerst	2. Anwendung statt Netzwerk	3. Recovery ist Fähigkeit
Die Sicherheitskette beginnt nicht am Gateway, sondern beim Menschen vor dem Rechner.	Post Zero Trust vermeidet unnötige allgemeine Netzwerkbeziehungen und stellt nur autorisierte Anwendungs- oder Kommunikationsbeziehungen bereit.	Backup allein genügt nicht; entscheidend ist die zuverlässige Wiederherstellung produktiver Umgebungen.

LEITGEDANKE	**Sicherheit beginnt mit der Identität – vor dem Rechner. Sie entscheidet vor dem Tunnel. Cyberresilienz endet erst mit gesicherter Wiederherstellungsfähigkeit.**

Post Zero Trust und Cyberresilienz

1. Sicherheit beginnt mit der Identität

Warum moderne Sicherheitsarchitekturen vor dem Rechner des Nutzers beginnen müssen – und erst mit der Wiederherstellungsfähigkeit enden.

Das klassische Sicherheitsmodell hat seine ursprüngliche Grundlage verloren: die Vorstellung eines vertrauenswürdigen internen Netzes und einer unsicheren Außenwelt.

Bevor wir darüber sprechen, auf welche Ressource ein Benutzer zugreifen darf, müssen wir grundsätzliche Fragen beantworten:

KERNFRAGE	**Wer sitzt überhaupt vor dem Rechner?**

Solange die Identität des Menschen nicht eindeutig festgestellt wurde, sollte weder eine geschützte Anwendung noch eine sicherheitsrelevante Kommunikationsumgebung oder ein Zugriffspfad in Richtung der Unternehmensinfrastruktur entstehen können.

Sicherheit beginnt deshalb nicht erst am Gateway. Sie beginnt auch nicht erst vor dem Tunnel.

KERNPUNKT	**Sicherheit beginnt mit der Identität – vor dem Rechner des Nutzers.**

Erst danach stellt sich die nächste Frage:

KERNFRAGE	**Warum sollte ein eindeutig identifizierter Benutzer überhaupt einen technischen Netzwerkzugang erhalten, wenn er für seine Aufgabe lediglich eine bestimmte Anwendung benötigt?**

Hier beginnt Post Zero Trust.

Und schließlich folgt die dritte Ebene:

KERNFRAGE	**Wie bleibt eine Organisation handlungsfähig, wenn trotz aller Schutzmaßnahmen Hardware, Infrastruktur, Daten oder sogar ganze Standorte ausfallen?**

Damit führt der Weg von der Identität über Post Zero Trust unmittelbar zur Cyberresilienz.

2. Die Sicherheitskette beginnt beim Menschen

Viele Sicherheitskonzepte beginnen mit dem Endgerät.

Doch auch ein abgesichertes Endgerät beantwortet zunächst nicht die wichtigste Frage:

Sitzt tatsächlich der berechtigte Mensch davor?

Aus unserer Sicht muss deshalb eine klare Reihenfolge gelten:

Zuerst die Identität. Dann die Sicherheitsumgebung. Dann die Policy. Dann die Anwendung. Und erst danach die Kommunikation.

Bei der technischen Umsetzung mit sayTRUST UZE – Universal Zero Trust Exchange – beginnt dieser Prozess auf der Client-Seite. Je nach Einsatzbereich kommt ein persönlicher hardwarebasierter oder ein gerätegebundener softwarebasierter UZE-Client zum Einsatz.

Besonders geschützte Hardware-Clients verfügen über einen mikroprozessorbasierten und AES-verschlüsselten Bereich und sind eindeutig ihrem vorgesehenen Besitzer zugeordnet. Der UZE-Software-Client wird fest an ein definiertes Gerät gebunden. Solange Identität, Client, Zertifikat und Berechtigung nicht erfolgreich geprüft wurden, bleibt die geschützte UZE-Client-Umgebung deaktiviert.

Der Besitz eines Hardware-Clients oder die bloße Verfügbarkeit einer Software-Client-Installation genügt damit nicht.

Gerät ein Hardware-Client in fremde Hände oder wird eine Software-Client-Installation kopiert, entsteht ohne die vorgesehenen Identitäts-, Zertifikats-, Geräte- und Berechtigungsprüfungen weder ein Zugang zu geschützten Anwendungen noch zur Infrastruktur.

KERNPUNKT	**Erst nach erfolgreicher Identitäts-, Client- und Berechtigungsprüfung wird der UZE-Client aktiviert. Erst dann steht die geschützte Sicherheitsumgebung zur Verfügung.**

Damit beginnt die eigentliche Sicherheitsentscheidung nicht am Client-Rechner, nicht im Rechenzentrum und nicht am Netzwerkzugang. Sie beginnt beim Menschen.

3. Vom geschützten UZE-Client in eine temporäre Laufzeitumgebung

Nach erfolgreicher Identitäts- und Client-Prüfung wird die geschützte UZE-Client-Umgebung aktiviert. Bei der hardwarebasierten Variante erfolgt dies aus dem AES-geschützten Bereich des persönlichen Client-Devices; die Softwarevariante wird aus der gerätegebundenen Sicherheitsumgebung gestartet.

Der UZE-Client arbeitet nicht einfach innerhalb einer gewöhnlichen lokalen Ausführungsumgebung weiter.

Stattdessen wird ein definierter Bereich des Arbeitsspeichers verschlüsselt und als temporärer Laufzeitkontext genutzt. Dort werden die für die Sitzung benötigten sicherheitsrelevanten Informationen sitzungsbezogen verarbeitet.

Dazu können beispielsweise gehören:

- Sitzungsparameter
- Policy-Informationen
- kryptografische Informationen
- Kommunikationsparameter
- temporär benötigte Routinginformationen

Diese Informationen müssen damit nicht dauerhaft auf dem lokalen System abgelegt werden.

Erst innerhalb dieses geschützten Kontextes beginnen die Policy-Prüfungen, die Sicherheitszustandsprüfungen des Endgeräts (Posture Checks) und die Kommunikationsprüfungen.

Die Reihenfolge lautet deshalb:

KERNPUNKT	**Identität → UZE-Client → geschützter RAM-Bereich → Policy- und Posture-Prüfung → UZE-Server → autorisierte Kommunikation.**

Sicherheitskette: vor dem Tunnel beginnt die Entscheidung

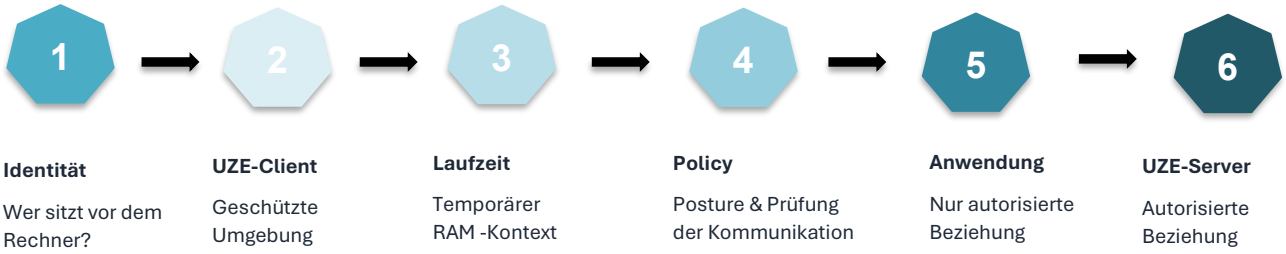

Abb. 1: Die technische Reihenfolge der Schutzkette.

Nicht umgekehrt.

4. Sicherheit muss vor dem Tunnel beginnen

Erst jetzt erreichen wir die nächste Sicherheitsstufe.

Auch nach erfolgreicher Identifikation darf nicht automatisch eine Kommunikationsverbindung aufgebaut werden.

Zunächst muss entschieden werden, ob die gewünschte Kommunikation überhaupt zulässig ist.

Dafür gilt ein einfaches Prinzip:

KERNPUNKT	**Erst Policy → dann Kommunikation.**

Noch bevor ein geschützter Kommunikationsweg entsteht, können unter anderem folgende Fragen geprüft werden:

- Welche Identität liegt vor?
- Welcher Benutzer ist dem UZE-Client zugeordnet und welche Client-Variante wird verwendet?
- Welches Gerät wird verwendet?
- Welche Anwendung soll kommunizieren?
- Welche Policy gilt für diese Anwendung?
- Welches konkrete Ziel darf erreicht werden?
- Welche parallelen Kommunikationswege sind während der Sitzung zulässig?
- Sind sämtliche für diese Sitzung definierten Voraussetzungen erfüllt?

Erst wenn die Sicherheitsentscheidung positiv ausfällt, darf der notwendige Kommunikationsweg entstehen.

Der Tunnel ist damit nicht der Beginn der Sicherheitsentscheidung.

KERNPUNKT	**Der Tunnel ist das Ergebnis einer bereits zuvor getroffenen Sicherheitsentscheidung.**

Sicherheit muss deshalb vor dem Tunnel beginnen. Aber sie beginnt noch früher:

KERNPUNKT	**mit der eindeutigen Identität des Menschen vor dem Rechner.**

5. Zero Trust war ein Meilenstein – aber kein Endpunkt

Das Grundprinzip von Zero Trust bleibt unverändert richtig:

KERNPUNKT	**Kein implizites Vertrauen allein aufgrund der Netzwerkposition.**

NIST SP 800-207 beschreibt Zero Trust als Architekturansatz ohne implizites Vertrauen aufgrund der physischen oder logischen Netzwerkposition beziehungsweise des Eigentums an einem Endgerät.

Post Zero Trust widerspricht diesem Prinzip nicht.

Im Gegenteil: Identität, Autorisierung und kontinuierliche Sicherheitsentscheidungen bleiben wesentliche Grundlagen.

Post Zero Trust stellt jedoch zusätzliche Architekturfragen.

Zero Trust fragt:

KERNFRAGE	**Wer darf unter welchen Bedingungen auf welche Ressource zugreifen?**

Post Zero Trust ergänzt:

KERNFRAGE	**Was muss für diesen Benutzer überhaupt sichtbar, adressierbar oder erreichbar sein?**

Und noch grundlegender:

KERNFRAGE	**Muss für die gewünschte Aufgabe überhaupt eine allgemeine Netzwerkbeziehung entstehen?**

6. VPN verbindet. Zero Trust kontrolliert. Post Zero Trust isoliert.

Der Unterschied liegt nicht in mehr Technik, sondern in der Architektur der Beziehung.

Abb. 2: Drei Architekturprinzipien im Vergleich.

Die Unterschiede lassen sich vereinfacht auf drei Architekturprinzipien reduzieren.

VPN: Der geschützte Weg ins Netzwerk

Ein VPN stellt eine verschlüsselte Verbindung zwischen einem Endgerät und einer entfernten Infrastruktur her.

Diese Verbindung kann stark verschlüsselt und mit mehrstufigen Authentifizierungsverfahren abgesichert sein.

Dennoch entsteht grundsätzlich eine Netzwerkbeziehung.

Damit muss anschließend geregelt werden, welche Systeme, Segmente und Dienste über diese Verbindung erreichbar sein dürfen.

Zero Trust und ZTNA: Der kontrollierte Zugriff

Zero-Trust-Architekturen verändern dieses Modell wesentlich.

Identität, Gerät, Kontext und Richtlinien bestimmen granular, auf welche Ressource zugegriffen werden darf. ZTNA kann dieses Prinzip für Anwendungszugriffe technisch umsetzen.

Die implizite Vertrauensstellung eines internen Netzwerks wird damit aufgehoben.

Je nach konkreter Implementierung kann jedoch weiterhin ein technischer Kommunikationspfad zwischen Client und Zielressource bestehen.

Post Zero Trust: Die Anwendung statt des Netzwerks

Post Zero Trust geht deshalb einen weiteren Schritt.

Der Benutzer erhält keinen allgemeinen Netzwerkzugang.

Stattdessen entsteht ausschließlich die für ihn autorisierte Anwendungs- oder Kommunikationsbeziehung.

Die dahinterliegende Infrastruktur bleibt gegenüber dem Client möglichst:

- unsichtbar
- nicht adressierbar
- nicht routbar
- nicht direkt erreichbar

Der Benutzer erhält damit keinen allgemeinen Netzwerkzugang. Aus seiner Perspektive arbeitet er ausschließlich mit der für ihn freigegebenen Anwendung.

KERNPUNKT	**Das ist ein fundamentaler Architekturunterschied.**

7. Nicht weniger Netzwerkzugang – sondern keinen allgemeinen Netzwerkzugang

Viele Sicherheitsarchitekturen verfolgen dasselbe Grundprinzip: Ein vorhandener Kommunikationsweg wird mit immer weiteren Schutzmechanismen abgesichert.

Authentifizierung, Segmentierung, Firewalls, Endpoint Protection, Network Access Control, PAM, Monitoring, SIEM und weitere Systeme können dabei wichtige Aufgaben erfüllen.

Doch Post Zero Trust stellt zunächst eine andere Frage:

KERNFRAGE	**Brauchen wir diesen Kommunikationsweg überhaupt?**

Was für die konkrete Aufgabe eines Benutzers nicht benötigt wird, sollte nicht nur blockiert, überwacht oder segmentiert werden.

Es sollte möglichst gar nicht erst Bestandteil seiner Kommunikationsarchitektur sein.

Damit wird Angriffsfläche nicht erst durch eine zusätzliche Sicherheitsschicht reduziert.

KERNPUNKT	**Sie wird bereits durch das Architekturdesign vermieden oder substanziell reduziert.**

8. Auch das Endgerät gehört zum Sicherheitsmodell

Der Arbeitsplatzrechner ist einer der kritischsten Punkte einer Remote-Access-Architektur – und auch innerhalb des unternehmensinternen Netzwerks ein besonders sensibler Bestandteil.

Er befindet sich unmittelbar in der Hand des Anwenders und häufig außerhalb der vollständig kontrollierten Rechenzentrumsumgebung.

Deshalb darf moderne Zugriffssicherheit nicht am Gateway enden.

Während einer sicherheitskritischen Sitzung muss auch betrachtet werden, welche parallelen Kommunikationsmöglichkeiten auf dem verwendeten Client bestehen.

Abhängig von der jeweiligen Policy können beispielsweise nicht benötigte:

- Browser
- Remote-Control-Anwendungen
- alternative Datenübertragungswege
- Bildschirmfreigaben
- sonstige parallele Kommunikationskanäle

für die Dauer der Sitzung kontrolliert oder eingeschränkt werden.

Das Ziel ist nicht, den Arbeitsplatzrechner des Benutzers permanent zu überwachen.

Das Ziel ist vielmehr, für die Dauer einer definierten sicherheitskritischen Sitzung eine kontrollierte Kommunikationsumgebung herzustellen.

Damit wird auch der Client selbst zum Bestandteil der Sicherheitsarchitektur.

9. Zero Footprint: Sicherheit darf keine unnötigen Spuren hinterlassen

Eine sichere Kommunikationsarchitektur sollte auf dem verwendeten Endgerät möglichst keine dauerhaft verwertbaren Informationen erzeugen.

Hier setzt das Zero-Footprint-Prinzip an.

Sicherheitsrelevante Sitzungsinformationen werden nur für die Dauer der jeweiligen Kommunikation benötigt.

Durch die Kombination aus einem geschützten UZE-Client und einer temporären geschützten Arbeitsspeicherumgebung können beispielsweise Sitzungs-, Routing- und kryptografische Informationen verarbeitet werden, ohne sie dauerhaft auf dem lokalen System abzulegen.

Nach Beendigung der Sitzung verliert dieser temporäre Kontext seine Funktion.

Das Ziel lautet:

KERNPUNKT	**Nach einer geschützten Sitzung sollen auf dem verwendeten Rechner möglichst keine verwertbaren Informationen über die geschützte Kommunikationsbeziehung zurückbleiben.**

Zero Footprint ist damit kein Komfortmerkmal. Es ist ein Sicherheitsprinzip.

10. Kryptografie ist notwendig – aber noch keine Architektur

Moderne Sicherheitsarchitekturen benötigen selbstverständlich leistungsfähige kryptografische und identitätsbasierte Verfahren.

Dazu können beispielsweise gehören:

- private PKI
- Multi-Faktor-Authentifizierung
- OTP
- SSO
- Gerätebindung
- digitale Zertifikate
- AES-Verschlüsselung
- Perfect Forward Secrecy
- rollen- und policybasierte Autorisierung
- kontrollierte privilegierte Zugriffe

Doch keine dieser Technologien allein bildet Post Zero Trust.

MFA ist nicht Post Zero Trust. PKI ist nicht Post Zero Trust. PFS ist nicht Post Zero Trust. Auch die Isolation einer Anwendung allein reicht nicht aus.

Entscheidend ist das Zusammenspiel aus:

KERNPUNKT	**Identität, geschützter Ausführungsumgebung, Policy, Kryptografie, Client-Kontrolle, Anwendungsisolation, Zero Footprint und der konsequenten Vermeidung unnötiger Netzwerkbeziehungen.**

Post Zero Trust ist deshalb kein einzelnes Feature.

KERNPUNKT	**Es ist ein Architekturmodell.**

11. Sicherer Zugriff allein ist noch keine Cyberresilienz

Abb. 3: Cyberresilienz verbindet Schutz, Verfügbarkeit, Datensicherheit und Wiederanlauf.

Bis hierhin betrachten wir vor allem die Sicherheit von Identität und Zugriff.

Doch selbst die bestmögliche Zugriffskontrolle beantwortet noch nicht eine weitere entscheidende Frage:

KERNFRAGE	**Was geschieht, wenn die zugrunde liegende Infrastruktur ausfällt oder ein Katastrophenfall eintritt?**

Cyberresilienz bedeutet deshalb mehr, als Angriffe zu verhindern.

Eine resiliente IT muss ihre wesentlichen Funktionen auch unter Störungen aufrechterhalten beziehungsweise innerhalb einer definierten Zeit zuverlässig wiederherstellen können.

Daraus ergeben sich vier zentrale Fragestellungen:

KERNFRAGE	**Wie verhindern wir unberechtigten Zugriff?**

KERNFRAGE	**Wie halten wir Anwendungen und Infrastruktur auch bei technischen Ausfällen verfügbar?**

KERNFRAGE	**Wie schützen wir Daten vor Manipulation, Verlust und Zerstörung?**

KERNFRAGE	**Wie stellen wir den Betrieb nach einem Katastrophenfall zuverlässig und schnell wieder her?**

Eine Sicherheitsarchitektur, die nur die erste Frage beantwortet, bleibt unvollständig.

12. Der „Tresor im Tresor“: mehrere Ebenen einer gemeinsamen Sicherheitsarchitektur

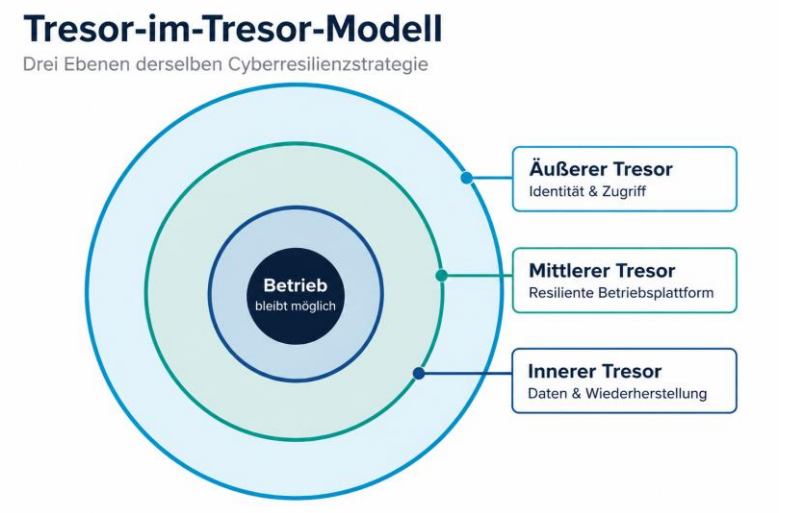

Abb. 4: Tresor-im-Tresor-Modell.

Drei Ebenen derselben Cyberresilienzstrategie

Eine cyberresiliente Infrastruktur lässt sich als mehrere ineinandergreifende Schutzbereiche betrachten.

Der äußere Tresor: Identität und Zugriff

Die erste Ebene verhindert, dass überhaupt unkontrollierte Kommunikationsbeziehungen entstehen.

Ein eindeutig identifizierter Benutzer, eine geschützte Sicherheitsumgebung und eine definierte Policy bilden die Grundlage dafür, dass eine Anwendung überhaupt kommunizieren darf.

Post Zero Trust sorgt anschließend dafür, dass Benutzer, Administratoren, externe Dienstleister oder Standorte nicht pauschal in interne Netze eingebunden werden.

Identität, Gerät, Anwendung und Policy entscheiden darüber, welche Kommunikation entstehen darf.

Der mittlere Tresor: die resiliente Betriebsplattform

Unterhalb der Zugriffsebene befindet sich die eigentliche Betriebsplattform.

Compute, Virtualisierung, Storage, Netzwerkdienste, VDI und weitere Infrastrukturservices müssen so aufgebaut sein, dass das Gesamtsystem innerhalb der definierten Ausfalltoleranz auch beim Ausfall einzelner Hardwarekomponenten oder vollständiger Nodes weiterarbeitet.

Der Ausfall eines Datenträgers, einer Netzwerkschnittstelle oder eines vollständigen Nodes darf innerhalb der vorgesehenen Redundanz- und Quorumkonfiguration nicht automatisch den Ausfall des bereitgestellten Dienstes nach sich ziehen.

Redundanz allein genügt dafür nicht.

Die unterschiedlichen Infrastrukturkomponenten müssen so zusammenspielen, dass Ausfälle automatisch abgefangen und verbleibende Ressourcen weiterhin genutzt werden können.

KERNPUNKT	**Resilienz muss Bestandteil der Betriebsplattform selbst sein – nicht erst Bestandteil eines Notfallplans.**

Der innere Tresor: Daten und Wiederherstellung

Auch eine hochverfügbare Infrastruktur kann einen Zustand erreichen, in dem Daten beschädigt, verschlüsselt oder gelöscht werden oder eine gesamte Betriebsumgebung nicht mehr nutzbar ist.

Deshalb bildet die Wiederherstellungsfähigkeit eine weitere eigenständige Schutzebene.

Backup, Restore, Auslagerung, Medienbruch, Live-Synchronisation (Live Sync) und Disaster Recovery müssen Bestandteil einer ganzheitlichen Resilienzstrategie sein.

Der entscheidende Punkt lautet:

KERNPUNKT	**Zugriffsschutz, Betriebsfähigkeit und Wiederherstellung dürfen nicht als drei voneinander unabhängige Projekte betrachtet werden.**

Sie sind unterschiedliche Ebenen derselben Cyberresilienzstrategie.

13. Backup ist eine Technologie – Recovery ist eine Fähigkeit

Viele Unternehmen verfügen über leistungsfähige Backup-Systeme.

Doch die entscheidende Frage lautet nicht:

KERNFRAGE	**Haben wir ein Backup?**

Sondern:

KERNFRAGE	**Wie schnell und zuverlässig können wir unseren Geschäftsbetrieb wiederherstellen?**

Zwischen einem erfolgreich geschriebenen Backup und einer erfolgreich wiederhergestellten produktiven Umgebung besteht ein erheblicher Unterschied.

Eine belastbare Wiederherstellungsstrategie kann deshalb unter anderem beinhalten:

- getrennte Fehlerdomänen
- kontrollierte Sicherungsketten
- Medienbruch
- Auslagerung
- Integritätsprüfungen
- regelmäßige Restore-Tests
- Live-Synchronisation
- definierte Wiederanlaufprozesse
- geografisch getrennte Betriebsmodelle

Damit wird aus einer Datensicherung eine tatsächliche Wiederherstellungsfähigkeit. Messbar wird sie durch verbindliche Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO), die regelmäßig überprüft werden.

KERNPUNKT **Backup ist eine Technologie. Recovery ist eine Fähigkeit.**

KERNPUNKT **Cyberresilienz benötigt beides.**

14. Resilienz muss getestet werden

Auch Hochverfügbarkeit darf nicht ausschließlich auf einem Architekturdiagramm existieren.

Eine belastbare Betriebsplattform muss zeigen können, was tatsächlich geschieht, wenn einzelne Komponenten ausfallen.

Beispielsweise:

- Was passiert beim Ausfall eines Hardwarebestandteils?
- Was geschieht, wenn ein kompletter Node abgeschaltet wird?
- Was passiert beim Ausfall einer Netzwerkkarte?
- Wie reagiert das System auf eine unterbrochene Netzwerkverbindung?
- Was geschieht beim Ausfall eines Switches?
- Wie verhält sich die Plattform beim Verlust eines Storage-Bereichs?
- Was passiert bei einem Standortausfall?
- Wie werden beschädigte Datenbestände behandelt?
- Wie schnell kann eine produktive Umgebung wiederhergestellt werden?

Erst regelmäßig wiederholte und dokumentierte Tests unter kontrollierten Bedingungen zeigen, ob aus einer theoretisch hochverfügbaren Infrastruktur eine tatsächlich resiliente Betriebsplattform geworden ist.

Gerade für kritische Infrastrukturen, öffentliche Einrichtungen und Unternehmen mit hohen Verfügbarkeitsanforderungen ist dieser Unterschied entscheidend.

15. Post Zero Trust und Cyberresilienz gehören zusammen

Damit entsteht eine durchgängige Sicherheitskette.

Identität schützt den Beginn. Nur ein eindeutig identifizierter Benutzer darf überhaupt eine Sicherheitsumgebung aktivieren.

Post Zero Trust reduziert die Angriffsfläche des Zugriffs. Nicht das Netzwerk, sondern die tatsächlich benötigte Anwendung beziehungsweise Kommunikationsbeziehung wird bereitgestellt.

Eine resiliente Betriebsplattform schützt die Betriebsfähigkeit. Innerhalb der definierten Ausfalltoleranz darf der Ausfall einzelner Hardwarekomponenten oder Nodes den laufenden Betrieb nicht unterbrechen.

Backup, Live Sync und Disaster Recovery sichern die Wiederherstellungsfähigkeit. Nach einem Katastrophenfall muss der Betrieb zuverlässig und möglichst schnell in einen definierten Zustand zurückgeführt werden können.

Diese Ebenen ersetzen sich nicht.

Sie ergänzen sich.

Genau darin liegt der Unterschied zwischen einer Ansammlung einzelner Security-Produkte und einer ganzheitlich gedachten Sicherheitsarchitektur.

16. Weniger Angriffsfläche statt immer mehr Schutzschichten

Über viele Jahre bestand eine typische Antwort auf neue Sicherheitsrisiken darin, zusätzliche Schutzkomponenten einzuführen.

Für eine neue Bedrohung kam eine weitere Technologie hinzu.

Für diese Technologie mussten anschließend Schnittstellen geschaffen, Berechtigungen eingerichtet, Updates gepflegt, Logs ausgewertet und neue Betriebsprozesse etabliert werden.

Dadurch ist in vielen Organisationen ein hochkomplexer Sicherheitsstack entstanden.

Doch Komplexität ist selbst ein Risiko.

Jede zusätzliche Schnittstelle kann ausfallen. Jede Fehlkonfiguration kann Schutzmechanismen umgehen. Jede Managementoberfläche benötigt Berechtigungen. Jede technische Abhängigkeit erschwert Wiederanlauf und Fehlersuche.

Deshalb sollte eine zentrale Frage moderner Sicherheitsarchitekturen nicht mehr nur lauten:

KERNFRAGE	**Welche zusätzliche Security-Komponente benötigen wir?**

Sondern:

KERNFRAGE	**Welche Angriffsfläche und welche technische Komplexität können wir durch eine bessere Architektur vermeiden oder substanziell reduzieren?**

Post Zero Trust setzt genau an diesem Punkt an.

17. Die praktische Umsetzung bei sayTEC

Bei sayTEC beschäftigen wir uns seit vielen Jahren mit der Verbindung von Zugriffsschutz und resilientem IT-Betrieb.

Mit sayTRUST UZE – Universal Zero Trust Exchange – werden Post-Zero-Trust-Prinzipien für kontrollierte Anwendungs- und Kommunikationsbeziehungen umgesetzt.

Die UZE-Architektur verbindet einen zentralen UZE-Server mit hardware- oder softwarebasierten UZE-Clients. Die Sicherheitskette beginnt mit der Identität des Benutzers. Erst nach erfolgreicher Identitäts-, Client-, Zertifikats- und Berechtigungsprüfung wird die geschützte UZE-Client-Umgebung aktiviert.

Darauf aufbauend entstehen der geschützte Laufzeitkontext sowie die notwendigen Policy- und Posture-Prüfungen. Erst wenn alle Voraussetzungen erfüllt sind, vermittelt der UZE-Server ausschließlich die autorisierte Anwendungs- oder Kommunikationsbeziehung.

Der Benutzer erhält keinen allgemeinen Netzwerkzugang. Interne Strukturen müssen gegenüber dem UZE-Client weder sichtbar noch frei adressierbar sein. UZE Plus überträgt denselben Architekturgrundsatz auf dedizierte Maschine-zu-Maschine- und Standort-zu-Standort-Kommunikation.

Mit sayFUSE HCI wird diese Zugriffsebene um eine resiliente Betriebsplattform ergänzt. Compute, Storage, Virtualisierung und Netzwerkfunktionen können innerhalb einer skalierbaren Infrastruktur bereitgestellt werden, deren Architektur bei entsprechender Redundanz-, Quorum- und Kapazitätsauslegung auf den Weiterbetrieb innerhalb definierter Ausfalltoleranzen ausgerichtet ist.

sayFUSE Backup ergänzt diese Umgebung um Backup-, Recovery-, Auslagerungs- und Disaster-Recovery-Szenarien.

Das Ziel ist dabei nicht, möglichst viele Technologien unter einem gemeinsamen Namen zusammenzuführen.

Das Ziel ist genau das Gegenteil:

KERNPUNKT	**Identität, Zugriff, Betrieb, Daten und Wiederherstellung von Beginn an als Teile derselben Sicherheitsarchitektur zu betrachten.**

18. Der eigentliche Paradigmenwechsel

Die Entwicklung der IT-Sicherheit lässt sich vereinfacht anhand einiger grundlegender Fragen beschreiben.

Das klassische Sicherheitsmodell fragte:

KERNFRAGE	**Wie schützen wir unser Netzwerk?**

Zero Trust fragte:

KERNFRAGE	**Wer darf unter welchen Bedingungen zugreifen?**

Post Zero Trust ergänzt:

KERNFRAGE	**Warum muss für diesen Zugriff überhaupt eine Netzwerkbeziehung entstehen?**

Doch aus unserer Sicht muss die Sicherheitsarchitektur noch einen Schritt früher beginnen:

KERNFRAGE	**Wer sitzt tatsächlich vor dem Rechner – und darf für diesen Menschen überhaupt eine sicherheitsrelevante Umgebung aktiviert werden?**

Cyberresilienz ergänzt schließlich:

KERNFRAGE	**Wie bleibt die Organisation auch bei technischen Ausfällen handlungsfähig – und wie stellen wir den Betrieb nach einem Katastrophenfall zuverlässig und schnell wieder her?**

19. Fazit: Sicherheit beginnt mit der Identität

Zero Trust bleibt eine zentrale Grundlage moderner IT-Sicherheit.

Post Zero Trust ersetzt dieses Prinzip nicht.

Es entwickelt die Architektur konsequent weiter.

Die Sicherheitskette beginnt jedoch bereits vorher.

KERNFRAGE	**Wer ist der Mensch vor dem Rechner?**

Erst nach erfolgreicher Identifikation darf eine geschützte Sicherheitsumgebung aktiviert werden.

Danach folgt eine klare Reihenfolge:

KERNPUNKT	**Identität vor Zugriff. Policy vor Kommunikation. Anwendung vor Netzwerk.**

Cyberresilienz erweitert diese Kette schließlich über den sicheren Zugriff hinaus:

KERNPUNKT	**Betrieb innerhalb definierter Ausfalltoleranzen. Schutz der Daten. Zuverlässige und schnelle Wiederherstellung nach einem Katastrophenfall.**

Eine belastbare Sicherheitsarchitektur entsteht nicht dadurch, jeden denkbaren Angriffsweg mit immer mehr Technik abzusichern.

Sie entsteht, wenn die Identität bereits darüber entscheidet, ob eine Sicherheitsumgebung aktiviert werden darf. Unnötige Kommunikationswege werden architektonisch vermieden; die verbleibende Infrastruktur wird so ausgelegt, dass definierte Ausfälle nicht automatisch zum Verlust der Betriebsfähigkeit führen.

KERNPUNKT	**Sicherheit beginnt mit der Identität – vor dem Rechner. Sie entscheidet vor dem Tunnel. Und Cyberresilienz endet erst mit der gesicherten Wiederherstellungsfähigkeit.**

Fazit

Identität	Isolation	Resilienz
Ohne eindeutige Identität darf keine sicherheitsrelevante Umgebung aktiviert werden.	Der Benutzer erhält keinen allgemeinen Netzwerkzugang, sondern arbeitet mit der autorisierten Anwendung.	Die Architektur muss definierte Ausfälle abfangen; die Wiederherstellung ist regelmäßig praktisch zu testen.

Der Paradigmenwechsel liegt nicht in einer weiteren Schutzschicht. Er liegt darin, unnötige Kommunikationsbeziehungen und technische Komplexität durch Architektur zu vermeiden oder substanziell zu reduzieren.