Universität St.Gallen
Institut für Wirtschaftsinformatik

Sicherheitsarchitekturen im Zeitalter von Zero Trust mit Fokus auf End-User

St.Gallen, Juni 2025

Prof. Dr. Peter Rohner, Sina Rohner & Joshua Auf der Maur

Management Summary

Zero Trust (ZT) gewinnt zunehmend an Bedeutung, doch bislang liegen nur wenige empirische Erkenntnisse zur konkreten Umsetzung in Schweizer Unternehmen vor. Diese Studie untersucht, wie grosse Organisationen zentrale ZT-Elemente wie digitale Identitäten, Authentisierung, Autorisierung, End-Point Security, qualifizierte elektronische Signatur und Verschlüsselung verankern und welche Massnahmen bereits umgesetzt oder geplant sind.

Im Gegensatz zu ZT wird das bisherige perimeterbasierte Sicherheitsmodell einer zunehmend vernetzten und cloudbasierten Welt nicht gerecht. Die vorliegende Studie macht deutlich, dass der Paradigmenwechsel hin zu ZT tiefgreifende Auswirkungen auf die Art und Weise hat, wie grosse Schweizer Organisationen wesentliche Mittel der Cyber Security im Bereich von End-User und End-Point (Frontend) handhaben.

Organisationen erkennen im Kontext von Cyber Security zunehmend, dass

- mit ZT die Identität zum zentralen Sicherheitselement wird,
- IAM-Systeme eine wesentliche Voraussetzung für die Umsetzung von ZT sind,
- kontextabhängige, kontinuierliche Authentisierung mit MFA zunehmend als notwendiger Standard angesehen wird, auch um SSO für eine nutzerfreundliche Authentisierung sicher einsetzen zu können,
- die Relevanz des Schutzes von End-Points in den Hintergrund tritt, dafür aber das Vertrauensniveau von digitalen Identitäten in den Vordergrund rückt,
- durch eine kontinuierliche Überprüfung von identitätsbasierten und Conditional Access Bedingungen, die als MFA kombiniert werden, Sicherheitsrisiken minimiert werden,
- Homeoffice (z.B. über VDI) und BYOD in einer ZT-Umgebung eine geringere Herausforderung darstellen, weil Zugriffe nicht mehr primär über den End-Point, sondern kontextbasiert gesteuert werden.

Konsequente Verschlüsselung von Daten stellt ein weiterer zentraler Baustein einer ZT-Architektur dar. Allerdings zeigt die Studie, dass viele Organisationen noch über kein ausgereiftes Datenklassifikationssystem verfügen. Im Zuge der verstärkten Nutzung von Cloud-Diensten, wie M365, gewinnt die Etablierung solcher Mechanismen an Relevanz.

Es zeigt sich, dass Organisationen, die ZT als strategisch relevantes Thema anerkennen und entsprechende Ressourcen bereitstellen, auch einen höheren technischen Reifegrad anstreben und damit ZT konsequenter umsetzen können.

ZT ist weit mehr als ein technologiegetriebenes Projekt. Es handelt sich um ein neues Sicherheitsparadigma, welches eine strategische Verankerung im Management erfordert. Für die Umsetzung von ZT bedarf es der Konzeption einer neuen Sicherheitsarchitektur.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

In einer zunehmend digitalisierten Welt stehen Organisationen aller Grössen und Branchen vor der stetig wachsenden Herausforderung, ihre Informationssicherheit zu gewährleisten. Dabei hat sich in den letzten Jahren ein Paradigmenwechsel im Bereich der Cyber Security vollzogen: weg von perimeterbasierten Verteidigungsstrategien hin zu einem Ansatz, der davon ausgeht, dass kein Akteur innerhalb oder ausserhalb des Netzwerks a priori als vertrauenswürdig angesehen werden kann. Dieses Konzept ist unter dem Begriff Zero Trust Architecture (ZTA) oder kurz Zero Trust (ZT) bekannt geworden und gewinnt weltweit, insbesondere in sicherheitskritischen Bereichen, zunehmend an Bedeutung (Rose et al., 2020).

ZT basiert auf der Annahme, dass Bedrohungen sowohl innerhalb als auch ausserhalb der traditionellen Sicherheitsgrenzen existieren. Besonders relevant ist dieser Ansatz in Bezug auf End-User, deren digitale Identität und Geräte für die Interaktion mit den digitalen Ressourcen des Unternehmens oftmals das Einfallstor für Angriffe darstellen. Wesentliche Mittel der Cyber Security, welche die End-User betreffen, sind digitale Identitäten, Authentisierung, Autorisierung, End-Point Security, qualifizierte elektronische Signatur (QES) und Verschlüsselung. Die Verantwortung für die korrekte Konfiguration und Nutzung der Mittel liegt gemeinsam bei den End-Usern / der Fachabteilung sowie der «first line of defense» in den IT-Abteilungen (bspw. IT-Admins, Security-Verantwortliche für Anwendungen und Infrastrukturen) (Institute of Internal Auditors, 2020).

Während sich zahlreiche Studien mit den theoretischen Grundlagen und technologischen Implikationen von ZT beschäftigen, fehlt es bislang an empirischen Untersuchungen zur praktischen, technologieunabhängigen Umsetzung dieses Konzepts. Es ist bisher unklar, in welchem Masse und mit welchen Mitteln ZT in Schweizer Organisationen mit Blick auf End-User tatsächlich implementiert wird und wie ZT architektonisch, organisatorisch, technisch in die «historisch gewachsenen» Strukturen von IT und Business eingebracht werden kann.

Forschungsfrage:

Wesentliche Elemente der Cyber Security liegen in der Hand der End-User und der benutzernahen «first line of defense». Es sind insbesondere das Management und die Anwendung von digitalen Identitäten, Authentisierung, Autorisierung, End-Point Security, qualifizierte elektronische Signatur (QES) und Verschlüsselung. Der Ansatz ZT bringt wesentliche architektonische, organisatorische und technisch Veränderungen mit sich. Wie gehen grosse Organisationen damit um?

Die vorliegende Studie adressiert diese Lücke, indem sie untersucht, wie grosse Schweizer Organisationen wesentliche Mittel der Cyber Security im Zeitalter von ZT einsetzen. Aufgrund der Komplexität von ZT erachten insbesondere grosse Organisationen ZT als

interne Angelegenheit, die nicht an externe Partner ausgelagert wird, weshalb grosse Unternehmen in dieser Studie betrachtet wurden. Der Fokus der Untersuchung liegt auf dem Management von End-Point und End-User Security.[1] Es wird einerseits aufgezeigt, welche Auswirkungen die befragten Organisationen durch ZT auf die bestehenden Ansätze der Sicherheitsarchitektur «vorne» (Frontend, insbesondere End-Point und End-User) antizipieren / erwarten (1). Andererseits wird aufgezeigt, welche Ansätze zur Umsetzung von ZT verfolgt werden. Die Analysen basieren auf der Erhebung von Ist-Zustand sowie Absichten / Plänen (2).

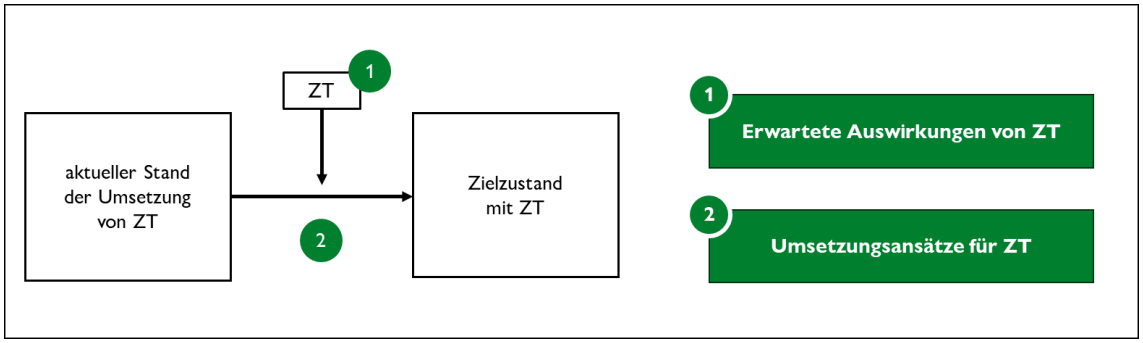

Abbildung 1 Scope der Studie

[1] Eine Folgestudie wird angestrebt, die sich mit der Umsetzung von ZT-Prinzipien im Bereich der Backend-Sicherheit sowie mit den Rollen und Verantwortlichkeiten der Second und Third Line of Defense im Rahmen ganzheitlicher Cyber-Sicherheitsarchitekturen befasst.

2 Konzeptionelle Grundlagen

Die Nutzung von Informationstechnologie (IT) ist zunehmend von Cloud-Diensten (SaaS), mobilen Endgeräten und Homeoffice-Szenarien geprägt. Angreifer, welche lokale Lücken im Frontend ausnutzen, stellen eine grosse Bedrohung dar (Kang, Li, & Cao, 2022). Das klassische, am Backend und damit am Perimeter orientierte Sicherheitsmodell stösst hier an seine Grenzen. Das Konzept von ZT ist als Antwort auf diese veränderten Rahmenbedingungen entstanden und stellt ein Sicherheitsparadigma dar, das sich durch eine konsequente Infragestellung von Vertrauen innerhalb und ausserhalb des Netzwerks auszeichnet (Rose et al., 2020, S. 2; NCSC, 2023, S. 2).

ZT basiert auf dem Grundsatz „never trust, always verify". Es wird dabei kein Akteur, weder innerhalb noch ausserhalb eines Netzwerks, a priori als vertrauenswürdig angesehen. Stattdessen wird der Zugang auf Ressourcen nur nach kontextabhängiger Authentisierung und Autorisierung, und dies bei jeder einzelnen Zugriffsanfrage neu, gewährt (Rose et al., 2020, S. 6; Phiayura & Teerakanok, 2023, S. 1). Dies spiegelt sich auch im ursprünglichen Konzept von Kindervag (2010, S. 2) wider, der betont, dass es im ZT-Modell keine Unterscheidung mehr zwischen vertrauenswürdigen und nicht vertrauenswürdigen Schnittstellen, Netzwerken oder Nutzern gibt. Vielmehr ist sämtlicher Netzwerkverkehr grundsätzlich als nicht vertrauenswürdig zu behandeln. Die Sicherheit solle in die „DNA des Netzwerks" eingebettet und „von innen nach aussen" gedacht werden, beginnend bei den zu schützenden Daten, nicht bei der Netzwerkperipherie (Kindervag, 2010, S. 2–6).

Wie das Nationale Zentrum für Cybersicherheit (NCSC) der Schweiz betont, geht es bei ZT weniger um ein starres Architekturmodell, sondern vielmehr um ein Sicherheitsprinzip, das auf den Selbstschutz von IT-Ressourcen abzielt, unabhängig von ihrer Position im Netzwerk (NCSC, 2023, S. 2–3). Damit einher gehen Konzepte wie Mikrosegmentierung, die dynamische Definition von Vertrauenszonen sowie die Etablierung von dezentralen Kontrollpunkten zur Durchsetzung von Zugriffsrichtlinien (Rose et al., 2020, S. 9; NCSC, 2023, S. 3).

Ein wesentlicher Aspekt dieser Studie ist die Einordnung der Umsetzung von ZT, wie oben erklärt, konzentriert auf das Frontend und damit auf die Security von End-User und End-Point (also allen Geräten, mit denen ein Nutzer direkt arbeitet oder die sich direkt mit einem Netzwerk verbinden), anhand eines Reifegradmodells. Es gibt verschiedene Modelle, eines davon ist das von Sarkar et al. (2022, S. 12) vorgeschlagene Zero Trust Maturity Model (ZTMM), das unterschiedliche Entwicklungsstufen von Organisationen auf dem Weg zur vollständigen Implementierung von ZT beschreibt, von einer perimeterbasierten Sicherheitslogik bis hin zu einer hochgradig automatisierten und verhaltensorientierten Sicherheitsarchitektur. Dieses Modell bietet eine strukturierte Grundlage zur Bewertung des technischen Implementierungsstandes von ZT-Massnahmen in Unternehmen. Das am meisten verbreitete ZTMM ist das der Cyber Security and Infrastructure Security Agency (CISA, 2023). Es ermöglich einen strukturierten Rahmen zur schrittweisen Umsetzung von ZT und bildet die Grundlage vieler anderer Modelle.

In dieser Studie wird der Begriff «Sicherheitsarchitektur» als ein Zusammenspiel technischer, architektonischer und organisatorischer Mittel verstanden, die darauf abzielen, die Integrität, Verfügbarkeit und Vertraulichkeit von IT-Ressourcen zu gewährleisten. Die in der Studie betrachteten Elemente werden direkt durch die End-User bedient, bzw. liegen in ihrer Verantwortung oder unmittelbaren Nutzung. Diese Elemente sind:

- Digitale Identität: Die digitale Identität ist ein Fundament von ZT. Sie repräsentiert eine eindeutige, überprüfbare Repräsentation einer natürlichen oder juristischen Person oder einer Maschine innerhalb eines IT-Systems und umfasst Attribute wie Benutzername, Zertifikate oder biometrische Daten (Lösser, Rohner, Kiselev, Wolfensberger & Winter, 2023, S. 4; Rose et al., 2020, S. 7). Im ZT-Kontext wird jeder Zugriff auf digitale Ressourcen nur dann gewährt, wenn die digitale Identität erfolgreich verifiziert und kontinuierlich bewertet wurde. Die Absicherung der digitalen Identität ist daher entscheidend für die Vertrauenswürdigkeit aller nachgelagerten Sicherheitsmechanismen (Kindervag, 2010, S. 2; Sarkar et al., 2022, S. 3). IAM, als System zur Orchestrierung bzw. Steuerung digitaler Identitäten, Rollen und Zugriffsrechte, welches zunehmend als Enabler für Cyber Security und digitale Geschäftsmodelle verstanden wird (Lösser et al ., 2023, S. 1–4), ist eine Voraussetzung für ZT. IAM umfasst Identitäts-, Authentisierungs- und Autorisierungsmanagement (Lösser et al., 2023, S. 4). Das ZTMM von CISA (2023) empfiehlt die Automatisierung von Just-in-Time- und Just-enough-Zugriffsentscheidungen, basierend auf individuellen Aktionen und Ressourcenbedarf (CISA, 2023, S. 14). Die Umsetzung zentraler, dynamisch aktualisierter Identitäts- und Zugriffsregeln wird als Ziel eines fortgeschrittenen Reifegrads betrachtet (CISA, 2023, S. 15).
- Authentisierung: Im ZT-Kontext ist Authentisierung ein kontinuierlicher, kontextabhängiger Prozess, der unter anderem auf Multi-Faktor-Mechanismen («Multifaktorauthentisierung» genannt, kurz MFA) basiert und eine laufende Bewertung der Vertrauenswürdigkeit verlangt (Rose et al., 2020, S. 5; NCSC, 2023, S. 3). Das ZTMM von CISA (2023) betont die Bedeutung phishing-resistenter MFA (z. B. FIDO2 oder PIV) und der kontinuierlichen Verifikation der Identität über die gesamte Dauer des Zugriffs (CISA, 2023, S. 14). Zusätzlich wird empfohlen, Authentisierungsverfahren mit Attributen wie Gerätezustand oder Nutzerverhalten anzureichern, um die Risikoabschätzung dynamisch zu gestalten (CISA, 2023, S. 14).
- End-Point Security: End-Points gelten als mögliche Einfallstore, auf die Angreifer ihre Angriffsvektoren richten und müssen deshalb aktiv in die Sicherheitsarchitektur eingebunden werden. Dies erfolgt über Monitoring, Device Posture Checks oder Mobile Device Management (Phiayura & Teerakanok, 2023, S. 2). Das ZTMM von CISA (2023) unterstreicht in diesem Zusammenhang die Notwendigkeit, den gesamten Lebenszyklus von Geräten, einschliesslich Provisionierung, Überwachung, Isolierung und Deprovisionierung, automatisiert zu steuern, um Compliance durchgängig durchzusetzen (CISA, 2023, S. 18). Dabei wird die Verknüpfung von Gerätezustand

mit Zugriffskontrollen als Schlüsselfaktor für adaptive Sicherheitsrichtlinien hervorgehoben (CISA, 2023, S. 17).

- Bring Your Own Device (BYOD): Die Integration privater Endgeräte in Unternehmenssysteme erfordert spezifische Sicherheitsmechanismen und stellt eine zentrale Herausforderung dar (NCSC, 2023, S. 2). Das ZTMM von CISA (2023) erkennt die begrenzte Kontrolle bei BYOD-Szenarien an und fordert daher Massnahmen wie Risikobewertung, eingeschränkten Zugriff auf Basis des Gerätezustands sowie die kontinuierliche Verifikation und Segmentierung von BYOD-Geräten (CISA, 2023, S. 16).
- QES: Eine QES sichert die Integrität und Authentizität digitaler Transaktionen und wird als ergänzende Vertrauenskomponente im ZT-Modell betrachtet (Rose et al., 2020, S. 22).
- Verschlüsselung: Verschlüsselung ist in ZT essenziell, sowohl für Daten „at rest“ als auch „in transit“, um Informationen auch bei einem etwaigen Zugriff durch nicht autorisierte Akteure zu schützen (Rose et al., 2020, S. 23).

Während digitale Identitäten, Authentisierung, Autorisierung und End-Point Security bei korrekter Konfiguration und Nutzung ZT befähigend wirken («ZT-enabling»), profitieren QES und Verschlüsselung von einer ZTA («ZT-benefitting»).

Abbildung 2 Bezug der Elemente zu ZT

Insgesamt wird mit ZT eine Minimierung impliziten Vertrauens sowie eine Maximierung kontextsensitiver Sicherheitsmechanismen angestrebt. Die genannten Elemente bilden gemeinsam die Grundlage einer dynamischen, anpassungsfähigen Sicherheitsarchitektur, welche der wachsenden Komplexität moderner IT-Umgebungen Rechnung trägt.

3 Vorgehen für die Studie

Zur Gewinnung eines vertieften Verständnisses über die Veränderungen, die ZT auf Ebene der End-User und der End-Points mit sich bringen, wurde in dieser Studie ein qualitatives Forschungsdesign gewählt. Diese Methodik erlaubt es, komplexe organisationsspezifische Charakteristiken, Wahrnehmungen und Handlungsweisen im Kontext von Cyber Security und ZT vertieft zu analysieren.

Die Datenerhebung erfolgte mittels semi-strukturierter Experteninterviews. Insgesamt wurden 18 grosse Schweizer Organisationen einbezogen, die unterschiedlichen Branchen angehören: Industrie (2), Banken (3), Logistik (2), öffentliche Verwaltung (6), Gesundheitswesen (2), Versicherungen (1) und Bildungswesen (1). Aus jeder Organisation wurden fachlich ausgewiesene Personen oder Teams befragt. Die befragten Experten bzw. Teams verfügen über vertiefte Kenntnisse in den Bereichen IT Governance, Informationssicherheit, Identity and Access Management (IAM), IT-Architektur und IT-Infrastruktur.

Die Interviews wurden jeweils durch ein Interview-Duo durchgeführt. Die Gesprächsführung erfolgte auf der Grundlage eines strukturierten Leitfadens, der eine konsistente Durchführung der Interviews sowie die vergleichbare Erhebung der relevanten Inhalte sicherstellte. Die Interviews wurden protokolliert und anschliessend durch eine systematische qualitative Inhaltsanalyse ausgewertet. Dabei stand insbesondere die Mustererkennung im Zentrum, um organisationsübergreifende Gemeinsamkeiten, Unterschiede sowie branchenspezifische Ausprägungen im Umgang mit ZT herauszuarbeiten.

4 Ergebnisse

Die Ergebnisse der Studie bieten einen empirischen Einblick in die Implikationen von ZT auf grosse Schweizer Organisationen mit Fokus auf End-User. In Abschnitt 4.1 wird aufgezeigt, welche Auswirkungen die befragten Organisationen durch den Einsatz von ZT auf ihre bestehenden Sicherheitsarchitekturen erwarten («1. Erwartete Auswirkungen von ZT»). In Abschnitt 4.2 werden typische Umsetzungsansätze beleuchtet, mit denen die Umsetzung von ZT verfolgt («2. Umsetzungsansätze für ZT»).

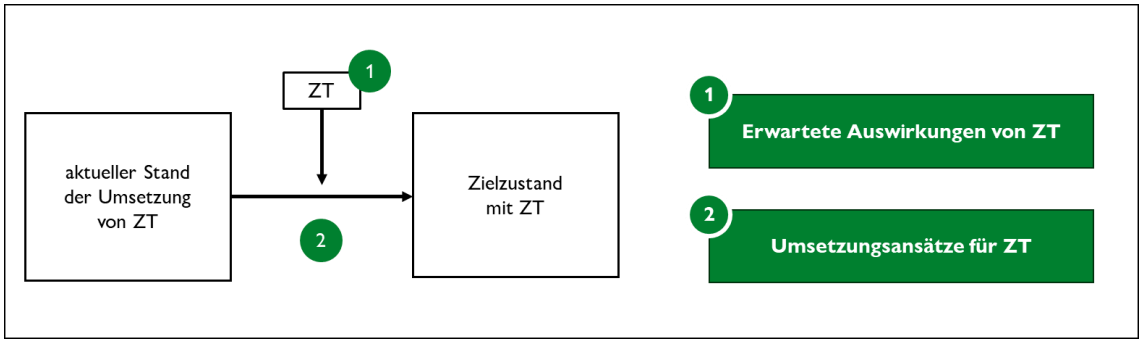

Abbildung 3 Ergebnisse der Studie

4.1 Erwartete Auswirkungen von ZT auf Elemente der End-User und End-Point Security

In diesem Abschnitt wird beleuchtet,

- welche Auswirkungen die befragten Organisationen durch die neue Denkweise mit ZT auf ihre bestehenden Sicherheitsarchitekturen mit Fokus auf End-User erwarten (Zielzustand mit ZT),
- inwiefern Veränderungen der Sicherheitsarchitektur im Hinblick auf End-User und End-Points aufgrund von ZT bereits integriert sind (aktueller Stand der Umsetzung von ZT),

bezogen auf

- digitale Identität,
- Authentisierung,
- Autorisierung,
- End-Point Security,
- QES,
- Ver- und Entschlüsselung.

4.1.1 Digitale Identität

Im bisherigen Perimeter-Sicherheitsmodell wurde die Identität an der Grenze zum Perimeter (Netzwerk) geprüft. Die Zone des Perimeters war und ist typischerweise gross (geht über eine Vielzahl von Anwendungen und IT-Infrastrukturobjekte hinweg). Ist der Zutritt in eine Zone einmal gewährt (bspw. durch Teilnahme oder via VPN-«Einwahl» in ein Segment), gilt ein «grundsätzliches Vertrauen» durch alle darin befindlichen Einheiten. Mit ZT wird neu die digitale Identität zur wesentlichen Verteidigungslinie. Ob ein End-Point bzw. End-User sich innerhalb oder ausserhalb des Perimeters befindet, ist nicht mehr der primäre Schutzmechanismus. Dieser basiert stattdessen auf Identität, Kontext und kontinuierlicher Überprüfung jeder Zugriffsanfrage.

Das Vertrauensniveau[2] der Identität gewinnt dadurch an Relevanz, bspw. AGOV-Qualität 100-600[3].

Aus den Interviews mit den befragten Organisationen konnten drei typische Szenarien, wie Identitäten entstehen, abgeleitet werden.

IAM-zentriertes Szenario
Für das User Life Cycle Management (join, promote, leave) inkl. dem Provisioning von Accounts zu den angeschlossenen Anwendungen ist eine IAM-Lösung im Einsatz. Die Identität entsteht im HR-System (bspw. SAP Success Factors) und wird (automatisiert) in das IAM überführt. Die Identitäten werden in zentralen Directories (deutsch: Verzeichnisdienst), bspw. Entra AD geführt, die mit dem IAM verbunden sind. Anwendungen verwalten keine Identitäten, sondern beziehen diese aus dem IAM. Die Zuweisung von Rollen und Berechtigungen erfolgt zentral in der IAM-Lösung, basierend auf vordefinierten Regeln und Attributen wie Organisationseinheit, Funktion oder Standort.

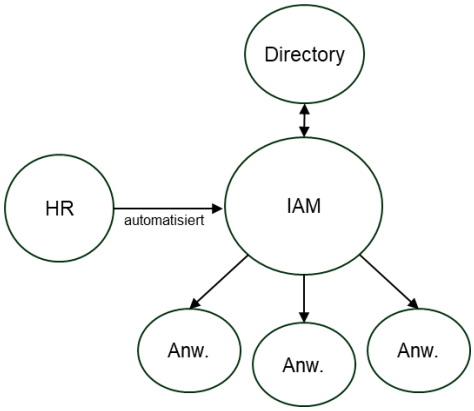

Abbildung 4 IAM-zentriertes Szenario

Directory-based Szenario
Für das User Life Cycle Management (join, promote, leave) inkl. dem Provisioning von Accounts zu den angeschlossenen Anwendungen ist ein Directory im Einsatz. Die Identität entsteht im HR-System (bspw. SAP Success Factors) und wird (automatisiert) in das

2 Englisch: Level of Assurance (LOA)

3 Siehe https://www.agov.admin.ch

Directory überführt. Die Rollenzuweisungen oder die Zuweisung von Berechtigungen erfolgt manuell. Anwendungen verwalten keine Identitäten, sondern beziehen diese aus dem Directory.

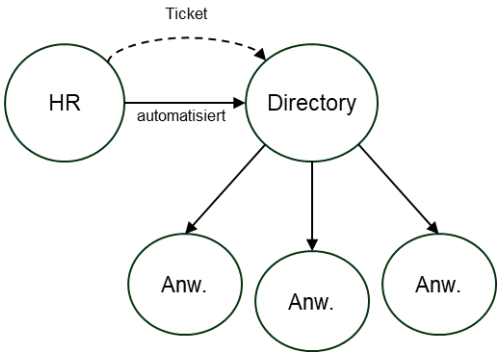

Abbildung 5 VD-zentriertes Szenario

Anwendungszentriertes Szenario
Das User Life Cycle Management (join, promote, leave) muss in jeder Anwendung separat betrieben werden. Die Identität entsteht über ein Ticket. Die Rollenzuweisungen oder die Zuweisung von Berechtigungen erfolgt manuell innerhalb der Anwendung.

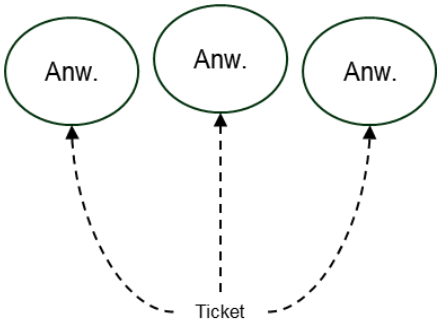

Abbildung 6 Anwendungszentriertes Szenario

Diese drei Szenarien werden in der Praxis kombiniert. Die meisten befragten Organisationen verfolgen ein Directory-based Szenario. Nur wenige haben ein IAM im Einsatz (IAM-zentriertes Szenario). Bei allen Organisationen gibt es Anwendungen, in denen die Identitäten direkt (bspw. für SaaS) verwaltet werden (Anwendungszentriertes Szenario), dies kommt unterschiedlich häufig vor. Das anwendungszentrierte Szenario ist nicht ZT-konform, da zentrale Steuerungs- und Kontrollmechanismen eingeschränkt sind und damit ein Sicherheitsrisiko besteht.

Um den Grundsätzen und Ansprüchen von ZT zu entsprechen, muss ein IAM mit hohem Grad an

- Organisation (User Life Cycle Management für Organisationen, Identitäten, Anwendungen, weitere Objekte),
- Integration (Connectors / Provisioning zu u.a. Anwendungen, Infrastrukturelementen) und
- Governance (Einbezug von Business und IT auf den unterschiedlichen Ebenen)

implementiert sein.

4.1.2 Authentisierung

Mit ZT gewinnt auch die Authentisierung von Anwendern (Menschen und Maschinen) an Bedeutung, indem statt einmal an der Grenze des Perimeters vermehrt für jede Anwendung, bzw. jeden Service authentisiert werden muss. Durch kontinuierliche Überprüfung von identitätsbasierten Faktoren und Conditional Access Bedingungen sowie durch MFA werden Angriffsvektoren reduziert. U.a. in Abhängigkeit des Szenarios der Identitätsverwaltung (IAM-, Directory-, applikationszentriert) erfolgt auch die Authentisierung unterschiedlich.

Single Sign-On (SSO) ermöglicht die Verwendung mehrerer Anwendungen nach einer Authentisierung und wird bei den meisten Organisationen eingesetzt. Eine Voraussetzung für SSO ist ein IAM- oder Directory-based Szenario.

Die meisten Organisationen regeln den Zugriff auf Anwendungen basierend auf dem bisherigen Perimeter-Sicherheitsmodell. Oft wird dazu einfache Authentisierung (1FA, typischerweise Passwort) eingesetzt. Vor dem Hintergrund von ZT ist dieser Ansatz nicht mehr ausreichend. Bei Cloud-Anwendungen oder Softwares (SaaS), welche nicht in den Zonen im eigenen Perimeter betrieben werden, wird häufig bereits 2FA eingesetzt. Die Verwendung von 2FA sollte jedoch primär vom Schutzbedarf der Anwendungen und nicht vom Modus bzw. Standort ihres Backends abhängen.

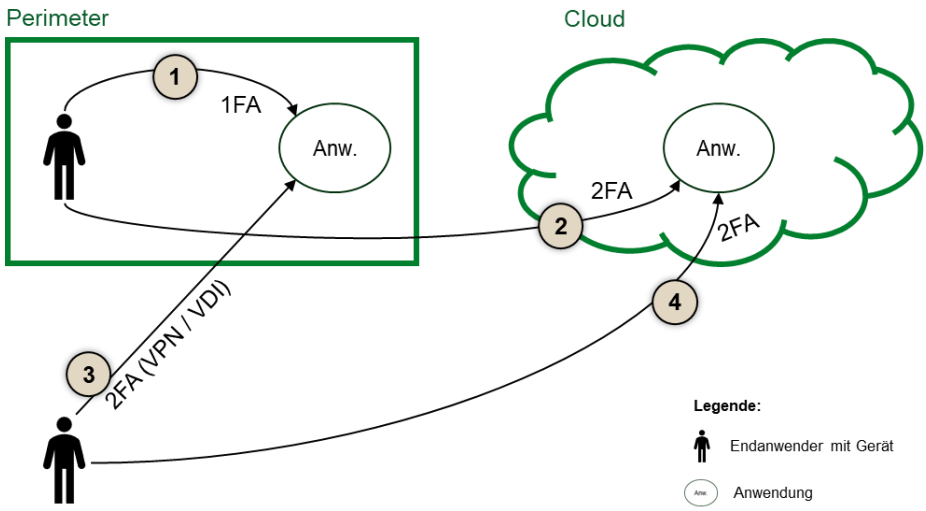

Abbildung 7 Anwendungen im Perimeter-Modell vs. im Cloud-Ansatz

Für die Authentisierung gibt es zwei unterschiedliche Arten von Prüfungen, welche die befragten Organisationen einsetzen. Identitätsbasierte Faktoren beziehen sich auf die direkte Verifizierung der Identität. Diese werden mit unterschiedlichen Mitteln überprüft. Conditional Access Bedingungen prüfen den Kontext einer Authentisierung.

- Identitätsbasierte Faktoren
    - Username
    - Passwort
    - Pin
    - Biometrische Daten
    - Zertifikat
    - One Time Code
- Mittel für die Prüfung der identitätsbasierten Faktoren
    - Authenticator App (bspw. MS)
    - SMS
    - FIDO (bspw. yubikey)
    - Smartcard
    - Badge (bspw. Fast User Switch)
- Conditional Access Bedingungen
    - Betriebssystem-Version
    - BYOD or not
    - Device Management or not (bspw. MDM)
    - Zeitbasiert
    - MAC Adresse
    - IP Adresse
    - Standort (geografisch)
    - Netzwerkzone
    - Netzwerk
    - VPN
    - Anomalie-Erkennung (ungewöhnliches Login-Verhalten, z. B. neue Länder, neue Geräte)

Ein bewusst gewähltes, klares und konsequent implementiertes Authentisierungskonzept (u.a. Prinzipien für Kombinationen aus Anwendungen und End-User- / End-Point-Situationen) ist notwendig für ZT. Die Authentisierung muss auf Identitäten mit hohem Vertrauensniveau basieren.

4.1.3 Autorisierung (Access)

Mit ZT ist Autorisierung neben Authentisierung ein zentrales Element zur Absicherung von Zugriffen. Zwei grundlegende Prinzipien spielen dabei eine zentrale Rolle: Least Privileged Access und Continuous Verification.

Das Least Privileged-Prinzip verlangt, dass jedem Benutzer, Mensch oder Maschine, nur die minimal notwendigen Berechtigungen für seine jeweilige Aufgabe zugewiesen werden. Continuous Verification sorgt dafür, dass ein Zugriff nicht nur einmalig vergeben wird, sondern laufend überprüft und gegebenenfalls angepasst oder entzogen wird, abhängig von Kontextfaktoren wie Nutzerverhalten, Gerätezustand oder Standort.

Viele der befragten Organisationen setzen das Least Privileged-Prinzip heute noch nicht konsequent um. Ein zentraler Hemmfaktor ist der hohe Aufwand für die detaillierte und fortlaufende Pflege von Berechtigungen. Statt einer granularen Rechtevergabe werden häufig sogenannte Referenzbenutzer verwendet, d. h. neue Nutzer erhalten Berechtigungen durch Kopie eines bestehenden, vergleichbaren Profils. Dieses Vorgehen reduziert den initialen Planungsaufwand, erhöht jedoch die Komplexität und Fehleranfälligkeit bei der operativen Umsetzung, insbesondere bei On- und Offboarding-Prozessen. Ein ZT-konformer Ansatz, der jedoch nicht häufig realisiert ist, wäre das rollenbasierte Berechtigungsmodell (Role-Based Access Control, RBAC). Bei RBAC werden Zugriffsrechte systematisch über Rollen modelliert und zentral verwaltet. Während die konzeptionelle Erstellung und Pflege von Rollenmodellen anfänglich aufwändig sein kann, ist die Umsetzung im operativen Betrieb, insbesondere bei Änderungen oder Benutzerwechsel, deutlich effizienter und nachvollziehbarer. RBAC ermöglicht zudem eine klare Trennung zwischen Basic Access (z. B. Basisrechte über IAM oder Directory) und Detailed Access (feingranulare Rechte innerhalb von Anwendungen).

Continuous Verification wird bei den meisten Organisationen nicht konsequent umgesetzt. Als Annäherung werden Logout und Session Timeout eingesetzt.

Für ZT bedarf es einer Grundautorisierung, die auf einem klaren Authentisierungskonzept basiert, sowie einer Feinautorisierung, die auf einem umfassenden Modell für die wesentlichen Anwendungen (unter Berücksichtigung von Nutzeranzahl, Schutzbedarf usw.) beruht.

4.1.4 End-Point Security

Bei den befragten Organisationen steht der Schutz von Geräten auch in einer ZTA nach wie vor im Fokus. Es haben sich die folgenden Grundszenarien für den Zugriff von Geräten auf Anwendungen gezeigt:

Gerät und Anwendung im Perimeter (1)
Bei den meisten befragten Organisationen ermöglicht die Authentisierung (1FA) am Gerät einen direkten Zugriff auf die Anwendung. ZT-konform wäre jedoch eine separate Authentisierung an den Anwendungen. SSO wird von den Unternehmen als userfreundlichen Ansatz gewählt. Durch starke Authentisierung, kontextbezogene Prüfungen und das Prinzip der minimalen Rechte kann SSO ZT-kompatibel gestaltet werden. Mikrosegmentierung wird als Zwischenlösung als Annäherung an ZT eingesetzt.

Gerät im Perimeter und Anwendung in der Cloud (2)
Bei diesem Fall verwenden die befragen Organisationen grundsätzlich 2FA. Als Good Practice für den Schutz der Informationen im Directory werden für Cloud-Applikationen zwei verschiedene Directories eingesetzt. Die Cloud-Applikation greift auf ein Directory

in der Cloud zu. Dieses Directory enthält nur wenige Attribute. Es verweist auf ein lokales Directory (führend), welches alle Attribute enthält (inkl. Passwort).

Gerät ausserhalb des Perimeters und Anwendung im Perimeter (3)
Meist wird entweder eine Verbindung zum Perimeter über VPN hergestellt oder das Gerät greift über die virtuelle Desktop Infrastruktur (VDI) auf Applikationen innerhalb des Perimeters zu. Danach wird der Zugriff auf Applikationen gleich gehandhabt, wie wenn das Gerät physisch innerhalb des Perimeters wäre.

Gerät ausserhalb des Perimeters und Anwendung in der Cloud (4)
Dieser Fall kommt in der Realität immer häufiger vor (SaaS-Anwendungen, Home Office / Workation). Wichtig ist in diesem Fall eine starke Authentisierung. Dies wird meist mittels 2FA umgesetzt. Da ZT grundsätzlich davon ausgeht, dass die Lokalisierung von Geräten bzw. Anwendungen für die Gewährung von Zugriffen nicht mehr genügt, sollten alle oben beschriebenen Fälle wie dieser behandelt werden.

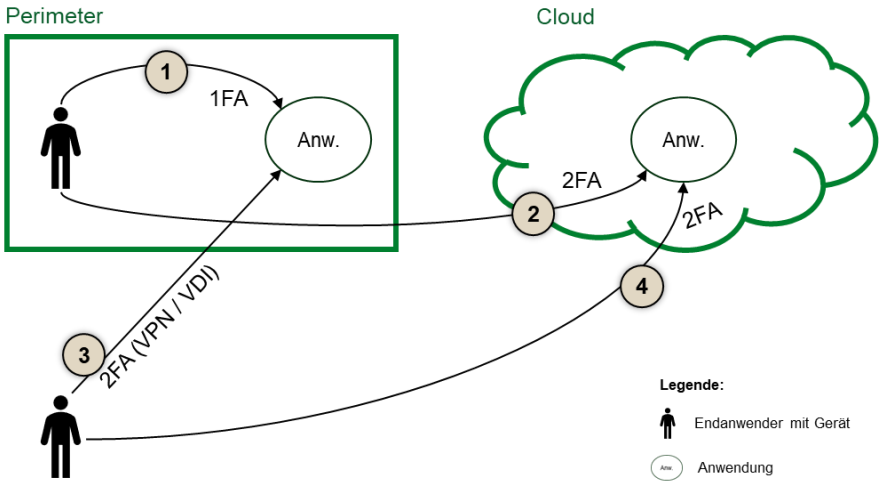

Abbildung 8 Vier Fälle des Zugriffs auf Anwendungen

BYOD
In nur wenigen der befragten Organisationen ist Bring Your Qwn Device (BYOD) zugelassen. Bei einer ZT-konformen Sicherheitsarchitektur wäre BYOD ähnlich sicher wie die eigenen Geräte der Organisation. Die Realität ist jedoch, dass der Schutz von Geräten insbesondere für den Zugriff auf Applikationen innerhalb des Perimeters noch sicherheitsrelevant ist. Oftmals wird mit BYOD nur der Zugriff auf Cloud-Applikationen ermöglicht. Als Good Practice wurde genannt, dass BYOD über VDI nach 2FA auf Anwendungen zugreifen können. Für Mobilgeräte wird, sofern überhaupt zugelassen, immer ein MDM eingesetzt.

Für den Umgang mit unterschiedlicher Lokalisierung von Geräten und Anwendungen, sowie mit BYOD bringt ein klares und konsequent umgesetztes End-Point-Security-Konzept den Schutz von Geräten in die Richtung von ZT.

4.1.5 Qualifizierte elektronische Signatur (QES)

In den befragten Organisationen werden für den *Benutzerservice* QES unterschiedliche Cloud-Applikationen (bspw. DocuSign, Skribble, Swisscom E-Sign) eingesetzt. In Organisationen des Service Public, welche die Infrastruktur des BIT (https://www.bit.admin.ch) nutzen, kann eine QES über die Smartcard erzeugt werden. QES benötigt eine stark geprüfte Identität sowie starke Authentisierung sowie ggf. die Prüfung nach ZertES. Nach ZertES müssen Anbietende von Zertifizierungsdiensten verschiedene Voraussetzungen erfüllen, um anerkannt zu werden wie bspw. im Handelsregister eingetragen zu sein.

4.1.6 Verschlüsselung

Der Bedarf an Verschlüsselung durch Benutzer wird von den befragten Organisationen meist als gering eingestuft. Im Kontext der Verwendung von Cloud Services, v.a. M365, wird die Frage, ob und welche Daten verschlüsselt werden sollten, bei einigen Organisationen virulent. Es werden dazu Klassifikationssysteme definiert bzw. im Falle von M365 von dort übernommen. ZT setzt voraus, dass heikle Daten unabhängig vom Speicherort (at rest, in transit, in use) verschlüsselt werden[4]. Die Kombination aus Klassifikation und automatisierter Verschlüsselung wird aktuell als Best Practice für Organisationen erachtet, die M365 verwenden und sich in Richtung ZT bewegen.

4.2 Umsetzungsansätze für ZT in der Praxis

In diesem Abschnitt wird zunächst die Ambition von Unternehmen in Bezug auf ZT betrachtet. Anschliessend werden zwei konkrete Beispiele aus der Praxis beschrieben.

4.2.1 ZT-Ambition

Die ZT-Ambition in Unternehmen wird anhand von zwei Dimensionen beschrieben. Eine der beiden Dimensionen beschreibt den ZT-Reifegrad basiert auf dem von dem ZTMM von CISA (2023). Diese umfasst drei technische Reifegrade zur Umsetzung von ZT. Die andere Dimension zeigt die geplanten organisatorischen Herangehensweisen, also die Investitionen und Projekte, die zur Umsetzung von ZT führen – von keinen ZT-Bestrebungen bis hin zu grossen, strategisch verankerten Programmen. Die befragten Organisationen wurden entlang dieser zwei Dimensionen in einer Matrix verortet.

[4] Einige Organisationen setzen zusätzliche Verschlüsselungstechnologien ein, um Daten in M365 unabhängig von Microsoft zu schützen. Ein potenzielles Risiko stellen Dokumente dar, die in SharePoint oder OneDrive abgelegt sind und die lokal (auf einen End-Point) synchronisiert werden. Zudem bleiben temporäre Dateien (tmp-Files), die beim Bearbeiten von Dokumenten auf einem End-Point entstehen, unverschlüsselt und stellen eine weitere potenzielle Sicherheitslücke dar. Organisationen, die sich Richtung ZT bewegen, sollten diese Lücken schliessen. In den befragten Organisationen werden spezialisierte SaaS-Lösungen wie Sepp Mail, HIN oder PrivaSphere genutzt, um den sicheren Austausch von sensiblen Informationen zu gewährleisten. Anstelle des direkten Versands von sensiblen Dokumenten wird zunehmend die Weitergabe von Links zu den gespeicherten Daten bevorzugt, um die Sicherheit zu erhöhen und unkontrollierte Weiterverbreitung zu verhindern. Zudem kommen in verschiedenen Szenarien sowohl symmetrische als auch asymmetrische Verschlüsselungsmethoden zum Einsatz.

Erste Dimension: Angestrebter ZT-Reifegrad (technisch, angelehnt an CISA, 2023)

Diese Dimension zeigt die technischen Reifegrade zur Umsetzung von ZT. Diese sind mit zunehmendem Reifegrad:

1. **Perimeter-Sicherheitsmodell:** Das Perimeter-Sicherheitsmodell basiert auf der Annahme, dass alles innerhalb des Perimeters (Netzwerk, Zone, etc.) vertrauenswürdig ist, während alles ausserhalb als potenziell gefährlich gilt. Der Ansatz war bisher vielerorts Status Quo, leistet aber keinen genügenden Beitrag zur Umsetzung von ZT, da wesentliche Prinzipien von ZT nicht erfüllt sind. Technisch charakterisiert sich dieser Reifegrad wie folgt:
    - Starke Trennung zwischen internem (trusted) und externem (untrusted) Perimeter
    - Einsatz klassischer Sicherheitskomponenten wie Firewalls, VPNs und IDS/IPS
    - Vertrauen basiert auf dem Standort (z. B. internes LAN) statt auf der Identität oder dem Kontext eines Zugriffs sowie wenig bis keine kontinuierliche Überprüfung von Identitäten oder Gerätezuständen
2. **Einzelne ZT-Mechanismen:** Die Einführung einzelner ZT-Mechanismen markiert den Übergang von perimeterbasierten Sicherheitsmodellen hin zu einem stärker identitäts- und kontextbasierten Schutzansatz. Der Einsatz neuer Mechanismen, die die Umsetzung von ZT begünstigen, wird ein höheres Sicherheitsniveau erreicht. Eine grundlegend neue Konzeption der Sicherheitsarchitektur findet nicht statt, wodurch ZT nicht vollständig erreicht werden kann. Technisch charakterisiert sich dieser Reifegrad wie folgt:
    - Einsatz von Mikrosegmentierung zur Begrenzung lateraler Bewegungen innerhalb des Perimeters
    - Nutzung eines IAM zur zentralen Verwaltung von Identitäten und Zugriffsrechten
    - Implementierung von Conditional Access Bedingungen
    - Einsatz von SSO
    - Klassifizierung und Schutz (bspw. Verschlüsselung) von Dokumenten basierend auf deren Sensitivität
3. **Neue ZT-Architektur:** Um die umfassende Umsetzung von ZT zu erreichen, bedarf es der Konzeption einer fundamental neuen Architektur. Im Zentrum steht nicht mehr der Perimeter, sondern die konsequente Durchsetzung von Zugriffskontrollen auf Basis von Identität, Kontext, minimalen Zugriffsrechten und kontinuierlicher Überprüfung. Der Schutz erfolgt von innen nach aussen, ausgehend von den zu schützenden Daten und Ressourcen, nicht mehr vom Perimeter. Technisch charakterisiert sich dieser Reifegrad wie folgt:
    - Einsatz von Zero Trust Network Access (ZTNA) zur durchgängigen, kontextbasierten Zugangskontrolle unabhängig vom Netzwerkstandort

- Zentrale Policy-Engines[5] zur durchgängigen Steuerung und Überwachung von Zugriffen auf Anwendungen, Dienste und Daten
- Starke Authentisierung und kontinuierliche Überprüfung von Identitäten
- Durchsetzung des Least-Privilege-Prinzips auf Nutzer-, Geräte- und Anwendungsebene
- Echtzeit-Inspektion und Logging des gesamten Datenverkehrs

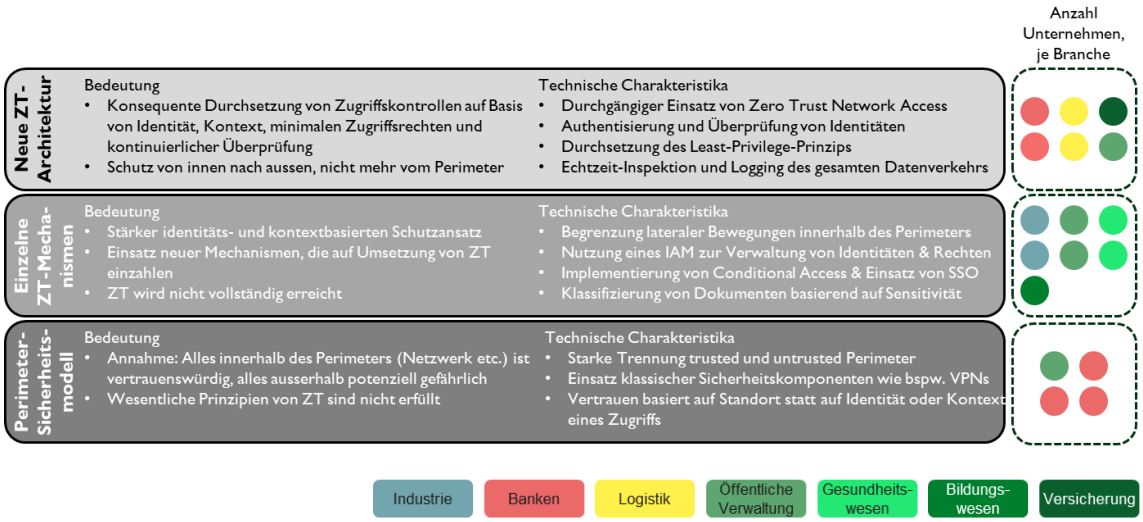

Abbildung 9 Angestrebte ZT-Reifegrade

Zweite Dimension: Investitionen und Projekte für ZT (organisatorisch)

Die andere Dimension zeigt die geplante organisatorische Herangehensweise zur Realisierung von ZT. Sie ist unterteilt in fünf Kategorien. Die Kategorien nehmen bezüglich der Ambition aufsteigend zu. Sie sind:

1. **Keine ZT-Bestrebungen:** Es bestehen, neben den gewohnten Aktivitäten rund um Security, keine Bestrebungen, ZT im Unternehmen umzusetzen. Das Thema findet weder auf strategischer noch auf operativer Ebene Beachtung.
2. **Erste Impulse bottom-up**: Einzelne, meist in IT oder Security angesiedelte Personen versuchen, die Relevanz von ZT im Unternehmen präsenter zu machen. Erste technische Massnahmen (bspw. Mikrosegmentierung) werden vereinzelt umgesetzt - ohne aktive Einbindung von Security-Gremien oder des Business.
3. **Opportunistische ZT-Bestrebungen:** ZT wird in thematisch angrenzenden Vorhaben berücksichtigt (bspw. Einführung eines IAM-Systems). Es gibt keine systematische Roadmap zur Erreichung von ZT.

[5] [1] Eine Policy-Engine trifft auf Basis vordefinierter Regeln kontextabhängige Entscheidungen über Zugriffe in einer Zero-Trust-Architektur.

4. **Gezielte ZT-Projekte**: Es gibt ein ZT-Projekt oder gar Programm, welches systematisch auf ZT hinwirkt. Für die Umsetzung von ZT wird die IT / Security als verantwortlich angesehen. Das Business ist wenig involviert.
5. **Verankerung von ZT:** Das Management erkennt ZT als zukunftsweisenden Ansatz für die Sicherheitsarchitektur des Unternehmens. Es werden mittel- bis langfristig genügend Ressourcen und Mittel bereitgestellt, um ZT im Unternehmen zu verankern.

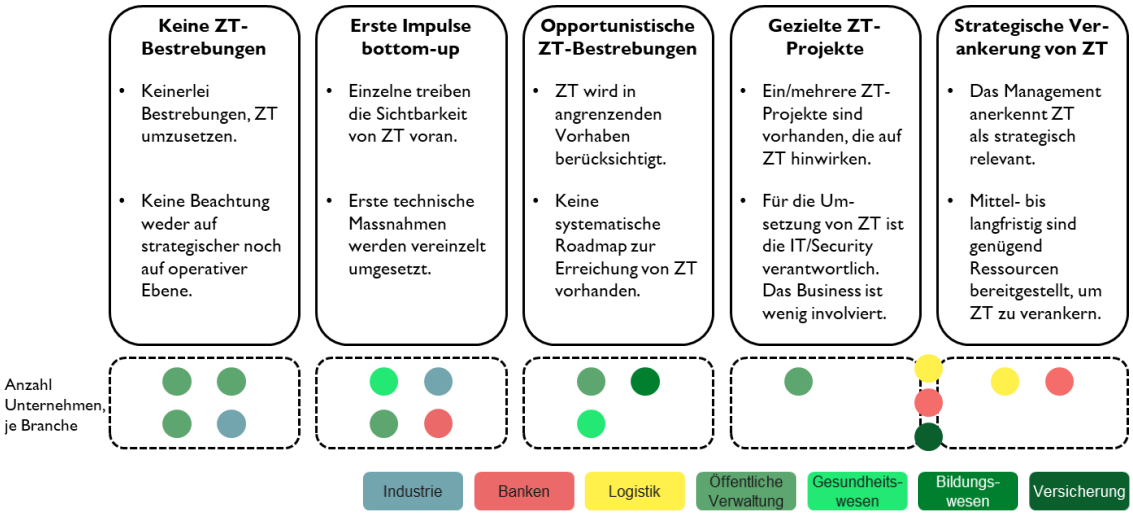

Abbildung 10 Investitionen und Projekte für ZT

Entlang dieser zwei Dimensionen sieht die Verortung der befragten Organisationen wie folgt aus:

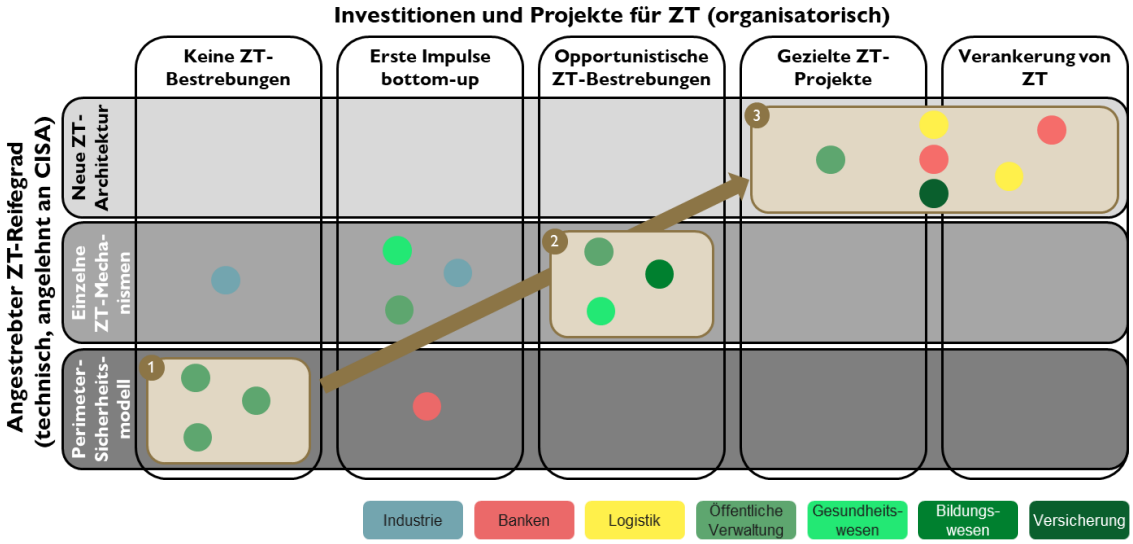

Abbildung 11 Verortung der befragten Organisationen in der Matrix

In der Matrix ist bezogen auf die befragten Organisationen eine Korrelation erkennbar, die zeigt, dass höhere Investitionen und Projekte für ZT (organisatorisch) mit einem höheren Anspruch an den technischen Reifegrad einhergeht. Daraus lässt sich schliessen, dass ein hoher technischer Reifegrad nur durch systematische Investitionen und Projekte

erreichen lässt. Zu überlegen ist, ob diese Korrelation (zumindest teilweise) einer Kausalität entspricht, bzw. ob ZT-Anstrengungen zu Umsetzungsfähigkeiten führen oder umgekehrt. Die Studie lässt keine abschliessende Antwort darauf zu. Zu erkennen sind jedoch drei Gruppierungen:

- **Gruppierung 1:** ZT wird weder strategisch noch operativ beachtet. Ein Perimeter-Sicherheitsmodell wird verwendet.
- **Gruppierung 2:** ZT wird opportunistisch in thematisch verwandten Projekten berücksichtigt, jedoch ohne eine systematische Roadmap. Dabei werden bspw. Mikrosegmentierung, IAM-Systeme oder Conditional Access Bedingungen implementiert.
- **Gruppierung 3:** Die Umsetzung von ZT erfolgt durch gezielte Projekte oder grosse Transformationsprogramme, welche eine neue ZT-Architektur implementieren.

4.2.2 Beispiele aus der Praxis

Im folgenden Abschnitt werden zwei unterschiedliche strategische Ansätze (Abgestimmte Investitionen und Projekte für ZT) zur Umsetzung einer ZTA beschrieben: zum einen der „Identität als Core"-Ansatz mit einem Fokus auf schrittweise technische Reife, zum anderen der langfristig ausgelegte „10+ Jahre"-Ansatz mit einem ganzheitlichen Transformationspfad bis 2032.

Praxisbeispiel «Identität als Core»
Diese beispielhafte ZT-Roadmap erstreckt sich über vier Jahre und verfolgt einen stufenweisen Ansatz zur Verbesserung der Cyber Security. Sie beschreibt die Entwicklung von einem physischen Perimeter-Sicherheitsmodell ("Physisch") über Mikrosegmentierung ("Netzwerk") hin zu einer ZT-Architektur, bei der die Identität das zentrale Element der Zugriffskontrolle bildet ("Identität"). Diese drei Stufen entsprechen im Wesentlichen den oben eingeführten technischen Reifegraden.

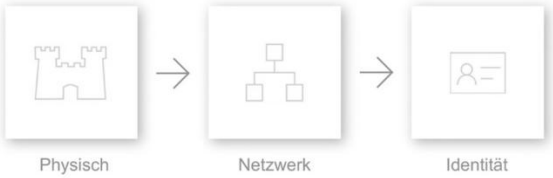

Abbildung 12 Ansatz des Praxisbeispiels "Identität als Core"

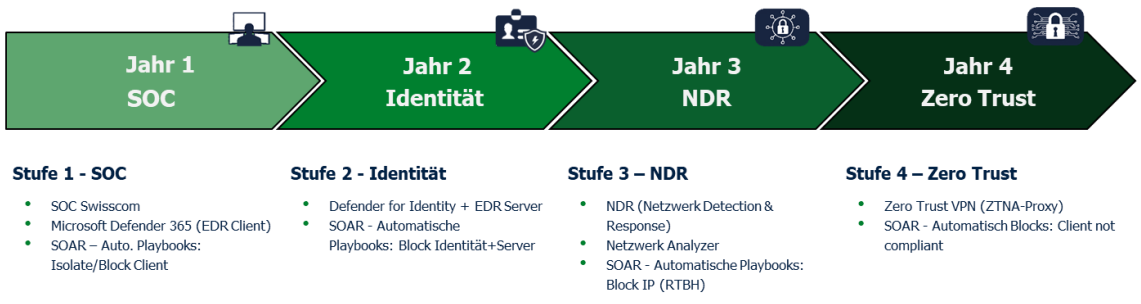

Abbildung 13 Roadmap des Praxisbeispiels "Identität als Core"

Im ersten Jahr liegt der Fokus auf dem Aufbau eines Security Operations Centers (SOC) sowie der Einführung von Microsoft Defender 365 mit EDR auf den Clients und automatisierten SOAR-Playbooks, um kompromittierte Clients schnell isolieren oder blockieren zu können. Im zweiten Jahr wird das Vertrauensniveau von digitalen Identitäten durch den Einsatz von Defender for Identity und bei den Servern sowie durch automatisierte Massnahmen zur Blockierung gefährdeter Identitäten und Server gestärkt. Im dritten Jahr folgt die Einführung von Network Detection & Response (NDR) zur besseren Erkennung von Netzwerkbedrohungen bei nicht verwaltetet Endgeräten (OT/IOT/usw.). Ergänzt wird dies durch Netzwerk Analyzer und automatische IP-Blockierung mittels SOAR. Im vierten Jahr wird ZT vollständig umgesetzt. Ein ZTNA-Proxy kontrolliert Zugriffe und nicht konforme Clients werden automatisch blockiert.

Praxisbeispiel «10+ Jahre»
Das Unternehmen geht methodisch vor, von PoC/PoV über skalierte Piloten hin zu produktionsreifen GA-Implementierungen. Technologische Schwerpunkte sind ZTE, NAAS, Microsegmentation sowie Schutz auf Workload- und Datenebene. Gleichzeitig werden Governance, Automatisierung und Prozesse eng mitentwickelt. Ziel ist ein vollumfängliches Zero Trust-Modell bis 2032.

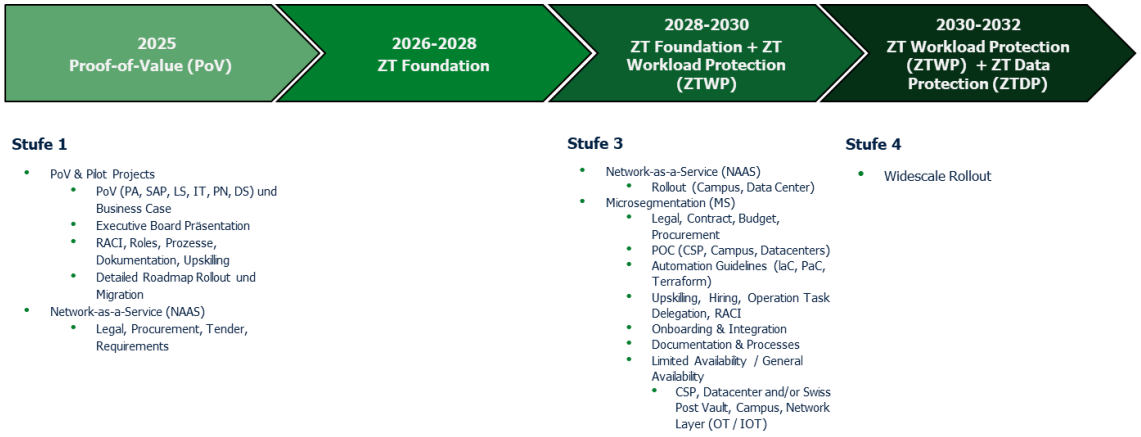

Abbildung 14 Roadmap des Praxisbeispiels "10+ Jahre "

Zwischen 2025 und 2032 wird stufenweise eine Zero-Trust-Architektur eingeführt. Im ersten Jahr stehen Proof-of-Value-Projekte und die Definition von Rollen, Prozessen und Anforderungen im Fokus. Von 2026 bis 2028 folgt der Aufbau der Zero-Trust-Grundlage mit Zero Trust Edge, automatisierten Richtlinien und ersten NAAS-Rollouts. In den Jahren 2028 bis 2030 wird Zero Trust Workload Protection (ZTWP) umgesetzt – inklusive technischer Einführung der Microsegmentierung und breiterem Rollout. Ab 2030 wird die Zero-Trust-Architektur mit der flächendeckenden Einführung von ZTWP und Zero Trust Data Protection (ZTDP) komplettiert, um Workloads und Daten ganzheitlich zu schützen.

5 Empfehlungen für Organisationen

Die im Rahmen der Studie gewonnenen Erkenntnisse aus den semi-strukturierten Interviews wurden mit den Teilnehmenden sowie weiteren Fachexperten validiert und diskutiert. Auf Basis dieser Ergebnisse wurden konkrete Empfehlungen erarbeitet, wie Cyber Security – insbesondere ZT – zur Stärkung des Business/IT-Alignments beitragen kann. Diese sind:

1. **Sense of Urgency schaffen**: Für die strategische Verankerung von ZT ist es zentral, ein Bewusstsein für die Dringlichkeit des Handelns zu schaffen. Das Erinnern an vergangene Sicherheitsvorfälle – insbesondere solche mit Auswirkungen auf das eigene oder vergleichbare Unternehmen – kann helfen, ein narratives Fundament für die Notwendigkeit von ZT zu legen. Eine emotional verankerte Dringlichkeit erhöht die Handlungsbereitschaft auf Managementebene.
2. **Finanziellen Nutzen durch einen «umgekehrten» Business Case verdeutlichen**: Um das Management von der Relevanz und dem Nutzen von ZT zu überzeugen, ist ein klarer finanzieller Mehrwert aufzuzeigen. Eine effektive Methode hierfür ist die Erstellung eines «umgekehrten» Business Cases: Anstatt den erwarteten Gewinn zu betonen, fokussiert dieser auf die Vermeidung von Kosten durch nicht eintretende Sicherheitsvorfälle. Die potenziellen finanziellen Schäden, die durch den Einsatz von ZT vermieden werden können, lassen sich quantifizieren und bieten so eine überzeugende Argumentationsbasis. Dies unterstreicht auch den möglichen Wettbewerbsvorteil durch erhöhte Resilienz.
3. **Business-Anforderungen als Treiber nutzen**: ZT sollte als Enabler für geschäftliche Innovationsbedarfe positioniert werden. Insbesondere in Kontexten, in denen aus Business-Sicht die Integration vielfältiger, neuer digitaler Lösungen angestrebt wird, kann ZT als Grundlage für sichere und rasche Implementierung argumentiert werden. Dadurch lässt sich die Relevanz besser vermitteln und die Akzeptanz steigern.
4. **Cyber Security näher ans Kerngeschäft bringen:** Eine wirkungsvolle Cyber Security erfordert organisatorische Nähe zum operativen Geschäft. Nur wenn die Sicherheitsbeauftragten eng mit den Geschäftsbereichen zusammenarbeiten, können sie reale Risiken frühzeitig erkennen und wirksame Massnahmen ableiten. Isolierte Sicherheitsstrukturen ohne Einbindung in operative Prozesse laufen Gefahr, an der Realität vorbei zu agieren.
5. **Weiterentwicklung der Rollenprofile im IT-Bereich**: Die Einführung von ZT bringt mittel- bis langfristig Veränderungen in den Anforderungen an IT-Fachkräfte mit sich. Es ist zu erwarten, dass der Bedarf an spezialisiertem Know-how für einzelne Technologien abnimmt, da sich die Sicherheitsarchitektur stärker auf standardisierte, ganzheitliche Ansätze konzentriert. Künftig werden breiter aufgestellte Kompetenzen benötigt, was auch die Rekrutierung von IT-Fachpersonal erleichtern kann. Entsprechend empfiehlt sich eine frühzeitige Überprüfung und Anpassung der Stellenprofile.
6. **Rollenverständnis neu ausrichten – vom Polizist zum Partner:** Die Sicherheitsverantwortlichen sollten sich als proaktive Dienstleister und Lösungspartner

positionieren. Ihre Aufgabe ist es, Sicherheit verständlich zu machen, Risiken konstruktiv aufzuzeigen und gemeinsam mit den Fachbereichen praktikable Lösungen zu erarbeiten. Ein begleitendes und erklärendes Vorgehen – statt punktueller Intervention – schafft Vertrauen und fördert eine konstruktive Zusammenarbeit.

7. **Etappenweise Umsetzung und kontinuierliche Kommunikation**: Der Weg zu vollständigem ZT sollte in klar definierte Etappen unterteilt werden. Diese schrittweise Vorgehensweise erleichtert die Planung, verbessert das Change-Management und erhöht die Akzeptanz im Unternehmen – sowohl bei Mitarbeitenden als auch beim Management. Kontinuierliche Kommunikation über Zielbild, Zwischenziele und Verantwortlichkeiten ist dabei entscheidend. Statt mit restriktiven Massnahmen zu agieren, ist ein erklärendes, unterstützendes Vorgehen zielführend – nach dem Prinzip: «Steter Tropfen höhlt den Stein».
8. **Interdisziplinäre Zusammenarbeit strukturell verankern:** Zur Entwicklung tragfähiger Sicherheitsstrategien empfiehlt sich die Etablierung eines interdisziplinären Gremiums oder Think Tanks. Dieses sollte Vertreterinnen und Vertreter aus Management, Technik, Recht und – wo sinnvoll – auch aus dem Business umfassen. Eine solche Zusammensetzung ermöglicht ganzheitliche Sichtweisen, reduziert Silodenken und fördert Innovation sowie Anschlussfähigkeit der Sicherheitslösungen.

6 Ausblick

Die Studie zeigt auf, dass ZT nicht nur ein technisches, sondern vor allem ein organisatorisches und strategisches Thema ist. Die gewonnenen Erkenntnisse helfen Unternehmen, Fachbereiche und Management für ZT zu sensibilisieren. Durch neue Formen der interdisziplinären Zusammenarbeit und dem Einsatz eines Think Tanks mit Vertretern aus Management, Technik und Recht können Organisationen eine fundierte Grundlage für eine erfolgreiche ZT-Implementierung schaffen.

Wie jede empirische Untersuchung unterliegt auch diese Studie bestimmten Einschränkungen. Die Befragung basiert auf einer relativ kleinen Stichprobe von lediglich 18 Organisationen, wodurch die Ergebnisse nur eingeschränkt generalisierbar sind. Zudem sind einige Branchen nur durch wenige Vertreter repräsentiert, was die Aussagekraft für einzelne Sektoren weiter begrenzt. Die entwickelten Empfehlungen stützen sich auf die Auswertung von Good-Practice-Beispielen und Erfahrungswerten, wurden jedoch im Rahmen der Studie nicht systematisch validiert, sodass keine belastbaren Aussagen über deren tatsächliche Wirksamkeit in der Praxis getroffen werden können. Darüber hinaus bezieht sich die Untersuchung ausschliesslich auf Organisationen in der Schweiz, wodurch länderspezifische Gegebenheiten und regulatorische Rahmenbedingungen die Übertragbarkeit der Ergebnisse auf andere Länder potenziell einschränken.

Die Studie hat zentrale Elemente der Sicherheitsarchitektur mit Fokus auf End-User vor dem Hintergrund von ZT beleuchtet. Es ergeben sich aus den bisherigen Erkenntnissen zahlreiche Ansatzpunkte für weiterführende Forschung. Ein zentraler Forschungsbereich betrifft die vertiefte Analyse der Hürden, die Unternehmen bei der Implementierung von ZT begegnen. Hier könnten insbesondere organisationsinterne Widerstände, fehlende Fachkompetenzen sowie technische Komplexitäten im Integrationsprozess näher untersucht werden, um differenzierte Handlungsempfehlungen für verschiedene Unternehmensgrössen und -branchen abzuleiten.

Ein weiterer wichtiger Aspekt zukünftiger Forschung liegt in der Identifikation und Validierung von Erfolgsfaktoren für eine erfolgreiche ZT-Implementierung. Neben technologischen Aspekten rücken hierbei zunehmend organisatorische und strategische Faktoren in den Vordergrund. Insbesondere die Bedeutung eines klaren Management Commitments, einer durchdachten Governance-Struktur sowie einer kontinuierlichen Sensibilisierung der Mitarbeitenden bedarf einer umfassenderen empirischen Fundierung.

Schliesslich eröffnet sich ein weiteres Forschungsfeld jenseits der Betrachtung von End-Usern und End-Points (Frontend) hin zum Netzwerk und dem Datenfluss (Backend).

Literaturverzeichnis

CISA. (2023). Zero Trust Maturity Model, Version 2.0. Cyber Security and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Institute of Internal Auditors. (2020, Juli). The IIA's three lines model – An update of the three lines of defense [PDF]. https://www.theiia.org/globalassets/site/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/glob-three-lines-model-paper_layout-rebuild.pdf

Kang, Z., Li, S., & Cao, Y. (2022). Probe the Proto: Measuring client-side prototype pollution vulnerabilities of one million real-world websites. In Proceedings of the 2022 Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2022.24308

Lösser, B., Rohner, P., Kiselev, C., Wolfensberger, A., & Winter, R. (2023). Identity und Access Management in grossen Schweizer Organisationen. Institut für Wirtschaftsinformatik, Universität St.Gallen (HSG). https://www.researchgate.net/publication/380360481_Identity_und_Access_MaManageme_in_grossen_Schweizer_Organisationen

Nationales Zentrum für Cybersicherheit (NCSC), & Eidgenössisches Finanzdepartement (EFD). (2023). Technologiebetrachtung: «Zero Trust»-Prinzip. https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/technologiebetrachtungen/Technologiebetrachtung-Zero-Trust-Prinzip-DE.pdf.download.pdf/Technologiebetrachtung-Zero-Trust-Prinzip-DE.pdf

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to Zero Trust Architecture. IEEE Access, 11, 19487–19509. https://doi.org/10.1109/ACCESS.2023.3248622

Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research Inc. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability, 14(18), 11213.