Best Practices für Cybersicherheit während der Post-Merger-Integration

WHITEPAPER

Einführung

Wenn Sie über die Einrichtung einer guten Infrastruktur in Ihrer gesamten Technologielandschaft nachdenken, ist die Cybersicherheit von größter Bedeutung. Wie Zscaler-Gründer Jay Chaudhry erklärt: „Unternehmen stehen eindeutig im Visier von Angreifern.“
Finanziell motivierte Cyberkriminelle führen Ransomware-Angriffe durch und erpressen Lösegeldsummen in Rekordhöhe von Unternehmen, die Betriebsunterbrechungen vermeiden wollen. Andere, darunter staatlich finanzierte Hacker, infiltrieren Unternehmen, um geistiges Eigentum und Geschäftsgeheimnisse zu stehlen und sich so einen kommerziellen Vorteil gegenüber der Konkurrenz zu verschaffen.

Darüber hinaus erleben wir regelmäßig, dass kritische Infrastrukturen Ziel von Cyberangriffen mit staatlicher Finanzierung werden, die als Schläferzellen fungieren und in Zeiten erhöhter Spannungen aktiviert werden können. Die Unternehmen sind in der Defensive. Diese Herausforderungen werden noch kritischer während einer Unternehmenstransaktion, wenn der Käufer bei der Integration seiner Akquisition durch die verschiedenen Komplexitäten der IT-Landschaft navigieren muss.

Forbes hebt dies in einem Beitrag zur wachsenden Bedeutung der Cybersicherheit bei Fusionen und Übernahmen[1]. „Unternehmen, die fusionieren, erwerben nicht nur neue Vermögenswerte und Marktchancen, sondern übernehmen auch die Cybersicherheitslücken und -risiken der Unternehmen, die sie in ihren Konzern aufnehmen. Unternehmen, die der Cybersicherheit von Anfang an Priorität einräumen, sind besser aufgestellt, um ihre Vermögenswerte zu schützen, ihren Ruf zu wahren und langfristig erfolgreich zu sein.“

[1] Forbes, The Growing Importance Of Cybersecurity In Mergers And Acquisitions, 7. Oktober 2024.

Cyberrisiken bei einer Fusion oder Übernahme

Lassen Sie uns etwas tiefer auf die allgemeinen Cybersicherheitsrisiken eingehen, die bei einer transaktionsbedingten Integration auftreten, um besser zu verstehen, wie man sie vermeiden kann:

1. Inkonsistenter Sicherheitsstatus

Risiko: Die fusionierenden Unternehmen verfügen wahrscheinlich über unterschiedliche Cybersicherheitspraktiken, –richtlinien und –technologien. Ein Unternehmen verfügt möglicherweise über starke Sicherheitsmaßnahmen, während das andere über schwächere Abwehrmaßnahmen oder veraltete Systeme verfügt.

Auswirkungen: Diese Inkonsistenz erhöht die allgemeine Anfälligkeit der fusionierten Unternehmen. Angreifer könnten die schwächeren Sicherheitssysteme eines der Unternehmen ausnutzen, um Zugriff auf beide zu erhalten.

2. Integration von IT–Systemen und Infrastruktur

Risiko: Die Integration verschiedener IT–Systeme (z. B. Netzwerke, Datenbanken, Cloud–Dienste) kann zu Lücken oder Schwachstellen in der Sicherheitsinfrastruktur führen. Legacy–Systeme sind möglicherweise nicht ausreichend gesichert oder entsprechen nicht den heutigen Sicherheitsstandards.

Auswirkungen: Diese Lücken könnten Cyberkriminellen als Einstiegspunkte dienen und möglicherweise vertrauliche Daten offenlegen oder den Geschäftsbetrieb stören.

3. Unsichtbare Schwachstellen in den Systemen des übernommenen Unternehmens

Risiko: Bei Due–Diligence–Prüfungen im Vorfeld von Unternehmenstransaktionen liegt der Schwerpunkt oft auf finanziellen, rechtlichen und betrieblichen Bewertungen, doch Cybersicherheitsprüfungen werden oft übersehen oder sind unzureichend. Versteckte Schwachstellen oder frühere Cyberangriffe werden möglicherweise erst nach Abschluss des Deals erkannt.

Auswirkungen: Wenn es in der Vergangenheit bei einem übernommenen Unternehmen zu Sicherheitsverstößen oder ungelösten Problemen gekommen ist, kann das erwerbende Unternehmen diese Risiken erben und sich unwissentlich Cyberbedrohungen aussetzen.

4. Risiken bei der Datenmigration

Risiko: Im Zuge von Fusionen und Übernahmen werden Daten häufig zwischen Systemen oder zentralen Plattformen übertragen. Dabei können vertrauliche Informationen preisgegeben werden, insbesondere wenn keine ordnungsgemäße Verschlüsselung und Zugriffskontrollen implementiert sind.

Auswirkungen: Vertrauliche Daten wie geistiges Eigentum oder Kundeninformationen können während der Übertragung abgefangen werden, was zu Datendiebstählen oder Sicherheitsverstößen führen kann.

5. Drittanbieter–Risiko

Risiko: Beide an einer Transaktion beteiligten Unternehmen unterhalten möglicherweise Beziehungen zu Drittanbietern, und die Integration dieser Anbieter kann neue Cyberrisiken mit sich bringen. Ein Verstoß bei einem Drittanbieter könnte die Sicherheit des fusionierten Unternehmens beeinträchtigen.

Auswirkungen: Ein Verstoß gegen das System eines Drittanbieters (z. B. Cloud–Hosting, Softwaretools) könnte sich auf das Unternehmen auswirken und kritische Daten offenlegen oder den Betrieb stören.

6. Mitarbeiterzugriff und Insider–Bedrohungen

Risiko: Mitarbeiter beider Unternehmen benötigen während des Integrationsprozesses möglicherweise Zugriff auf die Systeme und Daten des jeweils anderen Unternehmens. Die komplexe Verwaltung der Benutzerzugriffsberechtigungen kann Insidern (oder externen Angreifern, die Insider–Anmeldeinformationen nutzen) die Möglichkeit bieten, Systeme auszunutzen.

Auswirkungen: Unsachgemäß verwaltete Zugriffskontrollen könnten Mitarbeitern oder externen Akteuren den Zugriff auf vertrauliche Daten oder die Einschleusung von Schadsoftware ermöglichen, wodurch das Risiko eines Verstoßes steigt.

7. Erhöhte Angriffsfläche während der Umstellung

Risiko: Die Angriffsfläche vergrößert sich, wenn die Unternehmen zwei unterschiedliche Netzwerke, Systeme und digitale Assets zusammenführen. Diese größere Angriffsfläche bietet Hackern mehr Möglichkeiten zum Eindringen.

Auswirkungen: Das fusionierte Unternehmen ist während der Übergangsphase, in der Systeme und Prozesse noch integriert werden, möglicherweise einem erhöhten Risiko von Angriffen wie Phishing, Ransomware oder anderen Cyberangriffen ausgesetzt.

8. Kulturelle und operative Diskrepanzen

Risiko: Es kann zu einer mangelnden Kommunikation zwischen den IT- und Sicherheitsteams im neu fusionierten Unternehmen kommen. Unterschiedliche Sicherheitskulturen oder -prioritäten können zu einer Fehlausrichtung der Cybersicherheitsstrategien führen und so Lücken oder Konflikte verursachen.

Auswirkungen: Wenn die Cybersicherheitsrichtlinien nicht ordnungsgemäß zwischen den Teams abgestimmt oder kommuniziert werden, kann die Integration unbeabsichtigt Sicherheitslücken schaffen oder die allgemeine Cybersicherheitsstrategie untergraben.

9. Mangelnde Koordination der Vorfallsreaktion

Risiko: Das fusionierte Unternehmen verfügt möglicherweise nicht über einen einheitlichen, koordinierten Notfallplan. Die Prozesse zur Reaktion auf Cybervorfälle in den beiden Unternehmen können unterschiedlich sein, was die Erkennung und Eindämmung von Cyberangriffen erschweren und verzögern kann.

Auswirkungen: Mangelnde Vorbereitung kann im Falle eines Verstoßes zu längeren Reaktionszeiten führen, die Folgen verschlimmern und den verursachten Schaden potenziell vergrößern.

10. Risiken bzgl. der Einhaltung gesetzlicher Vorschriften

Risiko: In verschiedenen Regionen und Branchen gelten möglicherweise spezifische Compliance-Vorschriften für die Cybersicherheit (z. B. DSGVO, HIPAA, CCPA). Die Fusion zweier Unternehmen kann zu Versäumnissen oder Missverständnissen hinsichtlich der Einhaltung dieser Vorschriften in verschiedenen Rechtsräumen führen.

Auswirkungen: Bei Nichteinhaltung können Geldbußen, rechtliche Konsequenzen oder zusätzliche Kontrollen durch die Aufsichtsbehörden drohen, insbesondere wenn Kundendaten von einem Verstoß betroffen sind.

Wichtige Anforderungen und Anwendungsfälle für Cyber- und Netzwerkdesign

Bei einer fusionsbedingten Integration ist die Strategie für Netzwerkkonnektivität und -sicherheit ein entscheidender Faktor für die Geschäftsentwicklung des fusionierten Unternehmens. Die Gewährleistung gemeinsamer Cybersicherheitsstatndards bzw. -anforderungen ist von entscheidender Bedeutung, um die verschiedenen vorstehend erwähnten Risiken während einer PMI zu bewältigen, während die Netzwerkkonnektivität für die Geschäftsanforderungen unerlässlich ist. Diese Abwägung zwischen Risiko und Wertschöpfung liegt dem IT-Design und dem IT-Ansatz zugrunde, den das Unternehmen verfolgt.

Der wichtigste Aspekt einer fusionsbedingten Integration besteht darin, sicherzustellen, dass die IT-Systeme, Daten und Infrastrukturen sowohl des Erwerbers als auch des erworbenen Unternehmens bei der Vorbereitung auf die Integration sicher aufeinander abgestimmt sind.

1. Störungsfreie Behebung von Infrastrukturproblemen

Im Idealfall verfügen die beteiligten Unternehmen bereits vor dem ersten Tag über umfassende Kenntnisse der Netzwerkinfrastruktur des jeweils anderen Unternehmen, beispielsweise WAN, Firewalls, Switches, Router und Server, und haben eine schrittweise Problembehebung geplant, die den Geschäftsanforderungen entspricht. In der Praxis sind Netzwerkintegrationen oft sehr viel komplizierter und teurer, als bei der ursprünglichen Bewertung vorgesehen.

Für die zuständigen Fachkräfte ist es eine Herausforderung, ihre bestehenden Umgebungen bei der Weiterentwicklung aufrechtzuerhalten. Daher sind Tools und Lösungen, die Folgendes können, unbedingt erforderlich:

- Konnektivität zwischen zwei unterschiedlichen Netzwerken sicherstellen, um Zuverlässigkeit und Geschwindigkeit zu gewährleisten
- Integration bei minimaler Störungen der vorhandenen Netzwerkinfrastruktur

2. Lösungen für alle Konnektivitätsszenarien

Wenn Unternehmen im Zuge der laufendenIntegration auf neue Komplexitäten stoßen, lösen sie normalerweise jedes Konnektivitätsszenario, wie in Abbildung 1 gezeigt, mit einem temporären Netzwerkersatz, der separat entwickelt werden muss. Zu oft konzentrieren sich Lösungen wie VDI und VPN auf die Bereitstellung eines sicheren Zugriffs, obwohl diese Lösungen in den meisten Fällen die Netzwerke der beteiligten Unternehmen erweitern und die Angriffsfläche vergrößern. Darüber hinaus wird ihre Verwaltung und Skalierung zu einer Herkulesaufgabe, wenn das Unternehmen wächst oder neue Konnektivitätsszenarien (z. B. Zugriff von Drittanbietern oder Anbietern) entstehen. Wir stellen zunehmend fest, dass bei den IT-Designanforderungen der Schwerpunkt auf einer einheitlichen Plattform liegt, die sichere Konnektivität für alle Anwendungsfälle bietet und auf der Grundlage neuer Konnektivitätsmuster skaliert werden kann.

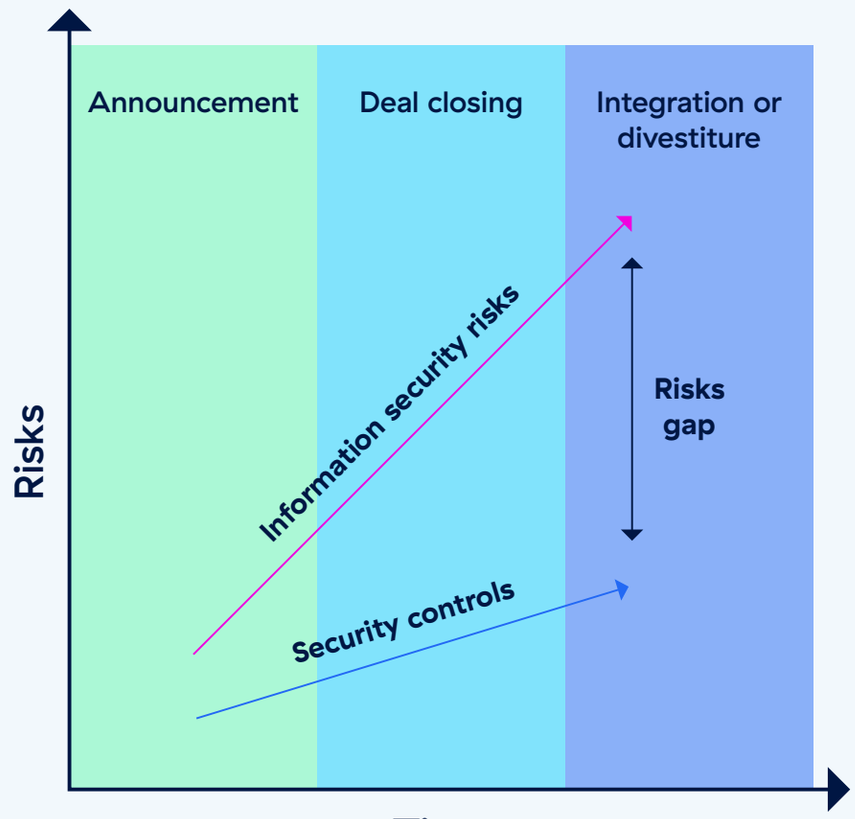
1. ANWENDUNGSFALL:

PARTEI	GERÄT	NETZWERK
Mitarbeiter des übernommenen/ übernehmenden Unternehmens	Laptop des übernommenen/ übernehmenden Unternehmens (unternehmensübergreifender Zugriff)	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
		Von Dritten kontrolliertes Netzwerk-Asset
Mitarbeiter des übernommenen/ übernehmenden Unternehmens	Laptop des übernommenen/ übernehmenden Unternehmens (nativer Zugriff)	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
		Von Dritten kontrolliertes Netzwerk-Asset
Netzwerkressource des Laptop des übernommenen/ übernehmenden Unternehmens	N/A	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
		Von Dritten kontrolliertes Netzwerk-Asset
Nicht-Arbeitnehmer / Dritt-User	Dritt-User / BYOD / Nicht verwaltet	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
	Laptop des übernommenen/ übernehmenden Unternehmens (unternehmensübergreifender Zugriff)	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
	Laptop des übernommenen/ übernehmenden Unternehmens (nativer Zugriff)	Vom übernommenen/ übernehmenden Unternehmen kontrolliertes Netzwerk-Asset
		Von Dritten kontrolliertes Netzwerk-Asset

3. Exposition erkennen und verhindern

Im Zuge der Unternehmenstransaktion, angefangen beim Screening und der Due Diligence bis hin zur Integration, werden die Lücken zwischen Sicherheitsrisiken und Kontrollen immer größer. Das von der fusionierten Unternehmen gewählte IT-Design sollte eine möglichst geringe Gefahr bergen, dass das Netzwerk eines Unternehmens Schwachstellen oder Bedrohungsvektoren einer anderen Einheit ausgesetzt wird.

Durch die Gewährleistung eines gemeinsamen Sicherheitsstatus/-standards zur Priorisierung der Risikominderung können alle Lücken, Schwächen oder Bereiche behoben werden, die verbessert werden müssen. Unternehmen bevorzugen IT-Lösungen und -Designs, die nicht nur die Angriffsflächen reduzieren, sondern auch proaktiv neue Angriffsflächen erkennen und rechtzeitig Bedrohungsinformationen liefern, wenn sich die Unternehmensumgebungen während der Integration ändern.



[1] Abb. 1: Cyberrisiken bei Unternehmenstransaktionen

4. Gewährleistung von Datenschutz und Privatsphäre

Während einer Integration werden Mitarbeiterdaten zwischen den Unternehmen ausgetauscht, Kundendaten konsolidiert, Lieferanten greifen auf neuere Datenumgebungen zu und Daten werden unternehmensübergreifend dokumentiert und klassifiziert. Angesichts der Auswirkungen von Verstößen oder Nichteinhaltung der Vorschriften müssen folgende IT-Designanforderungen erfüllt sein:

- Verschlüsselung vertraulicher Daten (sowohl während der Übertragung als auch im Ruhezustand), um unbefugte Zugriffe während der Integration zu verhindern
- Vorhandenes Framework zur Einhaltung der Datenschutzbestimmungen (z. B. DSGVO, HIPAA usw.)
- Bereitstellung von Überwachungs- und Prüffunktionen für den Datenzugriff
- Verhindern von Exfiltrationen während der Integration
- Sicherung aller Netzwerkkanäle durch einen einzigen Datenklassifizierungsstandard

5. Reibungslose und nahtlose User Experience

Mehrere Identitätszugriffsverwaltungssysteme, Inkompatibilität der Endusergeräte (z. B. Verwendung von zwei Laptops für den Zugriff auf die Unternehmensressourcen) und andere Probleme wie mehrere Authentifizierungsmechanismen (z. B. Dual-VPN) können die Userproduktivität beeinträchtigen und zu Verzögerungen bei der unternehmensübergreifenden Konnektivität führen. Unternehmen mit ausgereiften Integrationsstrategien wählen ein Design, das eine positive User Experience in den Vordergrund stellt und gleichzeitig sichere Konnektivität und Datenintegrität gewährleistet und Cyberbedrohungen verhindert. Im Idealfall wählen Unternehmen eine Lösung, die folgende Voraussetzungen erfüllt:

- Integration von Userrollen, Berechtigungen und sicherem Zugriff ohne unnötige Hürden
- Nutzung vorhandener Endgeräte, ohne dass ein sofortiger Austausch erforderlich ist
- Eliminiert die Notwendigkeit der Verbindung mit verschiedenen Lösungen/Ein- und Ausloggen, um Ressourcen im anderen Unternehmen zu erreichen

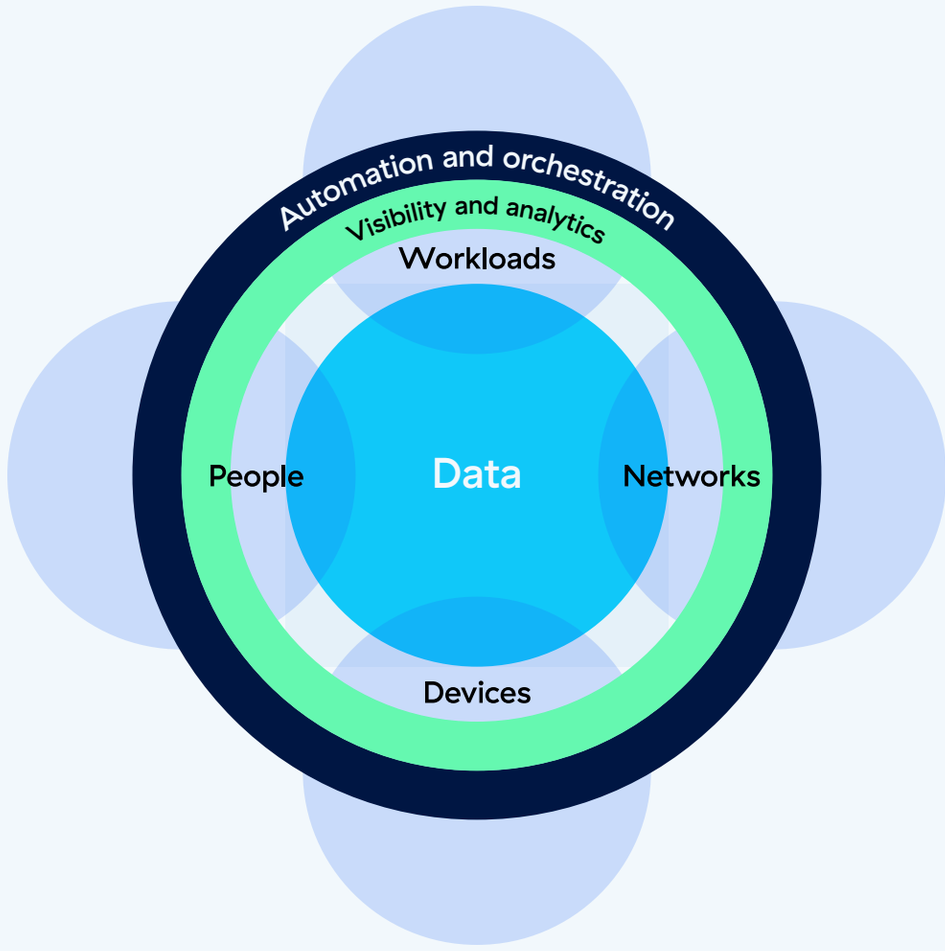
[1] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-ma-dont-drop-the-ball-Identify-and-reduce-cyber-risks-during-m-and-a.pdf

Um Ihren Wettbewerbsvorteil durch zahlreiche differenzierte Akquisitionen jedes Jahr aufrechtzuerhalten, ohne durch Integrationsineffizienzen, Kostenüberschreitungen und verpasste Meilensteine beeinträchtigt zu werden, müssen Sie die richtigen Designanforderungen auswählen und die Modernisierung der Technologie zum Eckpfeiler Ihrer Integrationsstrategie machen. Insbesondere wenn Sie die „unmögliche Dreifaltigkeit“ — niedrige Programmkosten, zeitnahe Ausführung und minimiertes Cyberrisiko — anstreben und gleichzeitig die Transformation und eine bessere User Experience vorantreiben möchten, können Sie sich nicht nur auf Playbooks verlassen, die sich hauptsächlich auf die Prozessoptimierung konzentrieren.

Das Zero-Trust-Modell für fusionsbedingte Integrationen

Immer mehr Unternehmen setzen auf ein Zero-Trust-Modell als Grundlage für die Designanforderungen für eine fusionsbedingte Integration. Das liegt daran, dass es alle Variablen umfasst, die während einer Integration zu Komplexität führen, und die Sicherheitsstandards erhöht.

Durch Implementierung eines Zero-Trust-Modells, bei dem der Zugriff auf Ressourcen auf jeder Ebene überprüft wird, werden laterale Bewegungen verhindert und sichergestellt, dass Sie während der Integration das bestmögliche Design erhalten. Ein Zero-Trust-Modell kann in drei Phasen implementiert werden:



[2] Abb. 2: Komponenten des erweiterten Ökosystems mit Zero Trust

PHASE 1: KRABBELN	PHASE 2: STEHEN	PHASE 3: LAUFEN
Schutz vor externen Bedrohungen, Zugriff auf webbasierte Anwendungen Authentifizierung mit mehreren Identitätsanbietern	Rollenbasierte Zugriffskontrolle über Proxy für private Unternehmensanwendungen	Nahtlose Migration für Workloads, IoT/OT usw.

Ein Zero-Trust-Modell trägt zur Beschleunigung fusionsbedingter Integrationen bei, indem es eine schnellere Wertschöpfung ermöglicht. Integrieren Sie nur die erforderlichen Komponenten, um von größtmöglicher Flexibilität zu profitieren Empfohlenes Vorgehen:

- Richten Sie innerhalb weniger Tage einen sicheren Zugriff für spezifische User, Anwendungen und Netzwerkressourcen ein
- Greifen Sie schnell und unkompliziert auf Unternehmensressourcen zu – für Cross-Selling, Innovationen und Unternehmensdienstleistungen (wie die Anbindung Ihres Lagers an das ERP-System, den Schutz geistigen Eigentums oder F&E)
- Reduzieren Sie die Gesamtauswirkungen im Falle von übernommenen Sicherheitsverstößen, indem Sie während der gesamten Übernahme einen Standardsicherheitsstatus durchsetzen. So können Sie den Usern die Produktivität ermöglichen, während Sie die Situation zuverlässig bewerten und auftretende Probleme beheben.

[2] https://www.forrester.com/blogs/when-it-comes-to-zero-trust-nobody-puts-appsec-in-a-corner/

Zscaler: Die führende Zero-Trust-Lösung für fusionsbedingte Integrationen

Zscaler eröffnet Unternehmen völlig neuartige Möglichkeiten zur Gewährleistung der Sicherheit und verkürzt fusionsbedingte Integrationen von neun bis 12 Monaten auf wenige Wochen. Indem Zscaler den Usern von AcquiredCo vom ersten Tag an Zugriff auf die Anwendungen gewährt, beschleunigt das Unternehmen die anfängliche Konnektivität, was wiederum die operative Konsolidierung beschleunigt und eine schnelle Wertschöpfung durch die Erzielung synergetischer Einnahmequellen durch das fusionierte Unternehmen ermöglicht. Zscaler legt außerdem Wert auf die kontinuierliche Überwachung der User- und Systemaktivitäten. Dies trägt dazu bei, potenzielle Datenschutzverletzungen zu verhindern.

Ein wichtiger Aspekt fusionsbedingter Integrationen ist die Abstimmung verschiedener Identitäts- und Zugriffsverwaltungssysteme. Mit Zscaler Zero Trust können Unternehmen bis zu 64 verschiedene SAML-Identitätsanbieter für den Internetzugang und bis zu 10 Konfigurationen für Single Sign-On (SSO) für den Zugriff auf private Unternehmensanwendungen verbinden. Dies ermöglicht die Integration von Usern mit mehreren IAMs, um einen konsistenten authentifizierten Zugriff in der fusionierten Infrastruktur zu gewährleisten. Darüber hinaus können AcquiredCo-User weiterhin ihre eigenen Geräte verwenden und so Zeit und Geld sparen, die mit der Bereitstellung neuer Hardware verbunden wären.

Einige der größten Unternehmen der Welt nutzen Zscaler und profitieren von folgenden Vorteilen:

- **Globalen, einheitlichen, sicheren und einfachen Zugang:**Die Fähigkeit, auf Anwendungen unabhängig von ihrem Standort zugreifen zu können, spielt eine geschäftskritische Rolle. Da sich Applikationen an verschiedenen Standorten befinden, sollten Sicherheits- und Zugangskontrolle auf alle Benutzer weltweit angewendet werden.

- **Erhöhte Sicherheit, Transparenz und Kontrolle:**Der gesamte Traffic-Fluss muss kontrolliert werden, um sicherzustellen, dass nur autorisierte Benutzer auf Anwendungen zugreifen können. Teams haben nun Einblick in alles, worauf Benutzer zugreifen, können bisher unbekannte Applikationen identifizieren und dann die entsprechenden Maßnahmen ergreifen.

- **Kostenvermeidung:** Sicherheits- und Netzwerkinfrastruktur, die einst dazu diente, Remote-Benutzern Zugang zu Ihrer Infrastruktur zu gewähren — und sie damit offenzulegen — kann im Rahmen dieses Projekts entfernt werden. Gleichzeitig können die Kosten für VPN, Netzwerkinfrastruktur und Softwareverwaltung minimiert werden.

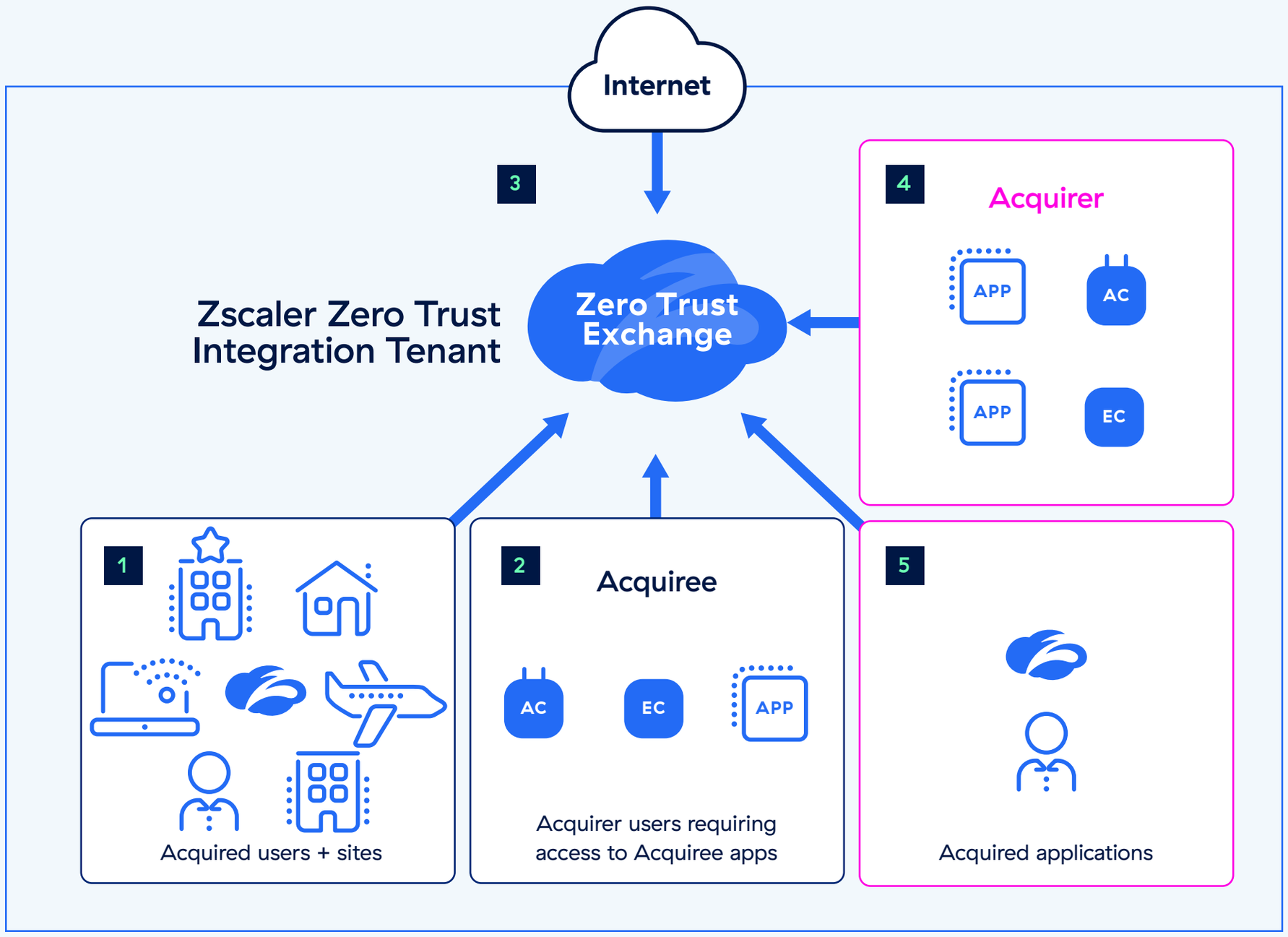
- **Cloud-Bereitschaft:** Wenn Anwendungen in die Cloud verlagert werden und User mobil sind, ist Sicherheit nur noch auf dem Endgerät oder in der Cloud möglich. Durch die Nutzung von Zscaler kann das übernehmende Unternehmen Cloud-Anwendungen ohne Infrastrukturbelastung einführen.

- **Abkopplung des Anwendungszugangs vom Netzwerk:** Wechseln Sie zu einem Modell des Anwendungszugriffs, das Identität und Stellung statt Netzwerkkonnektivität für den Zugang verwendet.

Careem, das erste Milliarden-Dollar-Technologieunternehmen im Nahen Osten und Zscaler-Kunde, erzielte erhebliche Ressourceneinsparungen (~55% Kostensenkung), die es in Transformationsinitiativen reinvestierte. Durch die Verwendung einer modernisierten Architektur mit Zscaler-Unterstützung konnte Careem auch geopolitische und Compliance-Komplexitäten bewältigen und Unternehmenstransaktionen vereinfachen.

1. bis 100. Tag mit Zscaler:

Zscaler ermöglicht einen sicheren und nahtlosen Zugriff während einer fusionsbedingten Integration. Anwendungen werden mit ausgehender Konnektivität mit Usern verbunden, ohne das Netzwerk für sie zu öffnen. Anwendungen sind niemals im Internet exponiert, da sie nicht auf eingehende Pings reagieren. Deshalb sind sie für unbefugte User völlig unsichtbar, was Cyberangriffe verhindert. Zscaler kann außerdem bisher unbekannte Anwendungen erkennen, die in AcquiredCo ausgeführt werden, und diese dann detailliert kontrollieren.



- **1. Schritt: Bereitstellung des Zscaler-Mandanten mit Domänen und DNS**
- **2. Schritt: Bereitstellen von Anwendungskonnektoren (Light VM-Agenten), um den Anwendungszugriff am ersten Tag vorzubereiten**
- **3. Schritt: Bereitstellen des Anwendungszugriffs ohne Konsolidierung mehrerer Identitätsanbieter**
- **4. Schritt: Bereitstellen von Client-Konnektoren für berechtigte User. Führen Sie eine Bedarfsanalyse durch, um die Anwendungsnutzung durch die User zu verstehen.**
- **Schritt 5: Korrelieren des Ist-Zustands für den Userzugriff auf Internet, Cloud und Anwendungen, um den Integrationsbedarf zu verstehen.**

Im Vorfeld der Integration können Sie nun die Anwendungserkennung in Acquiredco automatisieren und die Segmentierung von Einzelverbindungen zwischen Usern und Anwendungen starten, um den Zugriff auf kritische Anwendungen am ersten Tag ohne Verbinden von Netzwerken zu ermöglichen, und durch Bewerten des Risiko-Scores für erworbene Unternehmen den Datenschutz verbessern. Dazu gehören SSL-Prüfung, Inline-DLP und CASB, um vertrauliche Daten zu erkennen, Datenverluste zu verhindern und die Compliance wiederherzustellen. Darüber hinaus erhalten Sie Einblick in die User Experience und können Probleme proaktiv isolieren.

Im Zeitraum vom 1. bis 100. Tag ermöglicht Ihnen Zscaler, Auftragnehmern und Drittanbietern über BYOD und nicht verwaltete Geräte Anwendungszugriff zu gewähren. Sie können auch mit der Sicherung von Zweigstellen beginnen und die Konnektivität für IoT/OT-Geräte verbessern.

NAHTLOSE INTEGRATION MIT BEGRENZTEM IT-AUFWAND:

In bestimmten Fällen, in denen Sie keine Client-Konnektoren in AcquiredCo-Geräten einsetzen können, ermöglicht Zscaler dennoch die Integration über einen Cloud Integration ProxyTM. Dieser Proxy wird in einer Cloud-Umgebung implementiert, die in der Regel vom Käufer mit Zscaler App-Konnektor und Cloud-Konnektoren gesteuert wird. Durch eine einfache Änderung des Routings des Traffics von AcquiredCo auf diesen Proxy können alle User/Anwendungen/Workloads des übernommenen Unternehmens über die Zscaler Zero Trust Exchange™ mit den Ressourcen/Anwendungen des übernehmenden Unternehmens verbunden werden (oder umgekehrt). Für diese Methode müssen Sie keine Konnektoren auf AcquiredCo bereitstellen, um Zugriff zu erhalten. Dieser Ansatz eignet sich am besten für alle Zugriffsanforderungen für den 1. Tag. Sobald Sie mehr über die Geräte, Umgebungen und Infrastruktur von AcquiredCo erfahren, können Sie mit der Bereitstellung der anderen Komponenten wie zuvor beschrieben beginnen. Sobald Sie Komponenten bei AcquiredCo bereitgestellt und detaillierte Zugriffsrichtlinien und -kontrollen bereitgestellt haben, kann der Cloud-Integrationsproxy für die Anforderungen der nächsten Übernahme am ersten Tag verwendet werden. Lesen Sie mehr in unserem Lösungsprofil.

Zusammenfassung

Die Bewältigung der Cyber-Herausforderungen während einer fusionsbedingten Integration ist von entscheidender Bedeutung. Zu den Vorteilen der Implementierung von Zero Trust während fusionsbedingter Integrationen gehören eine Verringerung des Risikos von Datenpannen und Insider-Bedrohungen, eine Steigerung der Betriebseffizienz und eine reibungslose User Experience. Konkret gewährleistet Zscaler folgende Vorteile:

- **Schutz für alle User, Standorte und Anwendungen ab dem Tag der Vertragsunterzeichnung**
- **Schneller, sicherer und überprüfbarer Zugriff für beide Unternehmen ab dem 1. Tag**
- **Erstellung eines Profils für das übernommene Unternehmen, um angemessene Sicherheitskontrollen für interne/Internet-Anwendungen bereitzustellen**
- **Schnellere Umsetzung weiterer IMO-Prozesse (Anwendungen, Lieferkette, ERP)**
- **Vermeidung unnötiger Verzögerungen durch neue Infrastruktur, Telekommunikation und komplexe Infrastrukturintegrationen**
- **Eliminierung technologischer Überschneidungen und perspektivische Umstellung auf nutzungsbasierte Services**
- **Einfache Bereitstellung: Erfordert keine Hardware oder Hardware-Upgrades. Dies bedeutet eine sofortige Bereitstellung und Erkennung von Anwendungen, was zu einer besseren User Experience führt**

Bei Ihrer nächsten geplanten Unternehmenstransaktion beraten wir Sie gerne!

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.

+1 408 533 0288 **Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA** **zscaler.com/de**

zscaler™

Zero Trust Everywhere