

EBOOK

Navigieren am digitalen Horizont

Wie CIOs den Unternehmenserfolg durch die Harmonisierung von Technologie, Strategie und Resilienz vorantreiben



ESKER®

Was steht drin:

Einleitung

Der Schnittpunkt von Strategie und Technik.....3

Datensicherheit

Definieren, kontrollieren, beschränken..... 4

...und zertifizieren 6

Infrastruktur: Cloud Computing öffnet den Himmel

Zuverlässigkeit, Monitoring, Skalierbarkeit & Redundanz 7

Agile Methodik..... 9

Nahtlose Konnektivität

Integration, Integration, Integration 10

Fazit

Mehr als Einzellösungen: Eine globale Plattform zum Schutz von Daten
und zur Skalierung von Abläufen 12

Über Esker 13

Der Schnittpunkt von Strategie und Technik

Der CIO und das Team für Informationssysteme (IT) sind in den letzten Jahrzehnten über das operative Geschäft hinaus zu einem integralen Bestandteil der Unternehmensstrategie geworden. Sie installieren nicht mehr einfach nur Software auf den Computern und reparieren Drucker, sondern sie sind jetzt ein aktiver Teil der Antizipation und Planung zur Sicherung der Geschäftskontinuität. Zu den Veränderungen, die sich in den Unternehmen vollziehen, gehören Themen wie:



Auf dem Weg zur digitalen Transformation



KI wird in Business-Anwendungen zunehmend zur Norm



Regulatorische Einbeziehung hinsichtlich der Spezifikationen für die Datenerhebung



Bedrohung für die Cybersicherheit

Was steht in diesem E-Book?

Durch diese Faktoren wird die Aufgabe des CIO zu einer strategischen Aufgabe, bei der es darum geht, die Cyber- und Datensicherheit zu gewährleisten und gleichzeitig intern für Einheitlichkeit und Konsistenz zu sorgen. Diese Art der strategischen Planung erfordert einen Schritt zurück, um das Gesamtbild zu sehen, damit Entscheidungen mit Bedacht und Weitsicht getroffen werden können. Da Cyber- und Datensicherheit zu den Kernwerten eines Unternehmens gehören sollten, müssen sich CIOs für Lösungen entscheiden, die zuverlässig, stabil und widerstandsfähig sind. In diesem E-Book finden Sie einige Tipps und Tricks, die Sie bei der Einführung neuer Software und neuem IT-Equipment in die richtige Richtung lenken sollen.

Die vom IT-Team betroffenen Entscheidungen haben sehr reale Auswirkungen auf alle Geschäftsbereiche.

Nicolas Bragard
Esker CIO

Datensicherheit

Definieren, kontrollieren, beschränken

Ein weltweites Netz von strategisch platzierten Produktionsstätten und Rechenzentren vereint sowohl die physische als auch die virtuelle Infrastruktur. Eine solche Gesamtstruktur bietet ein hohes Maß an Sicherheit, Flexibilität und Leistung und hilft Ihnen, vertrauliche Informationen zu schützen. Die Sicherheitsmaßnahmen für Automatisierungslösungen lassen sich grob in drei verschiedene Dimensionen einteilen: plattforminhärente, externe Kommunikationssicherheit und interne Zugangskontrollen.

1

Plattforminhärente Sicherheitsmaßnahmen umfassen:

- Redundante Firewalls, SIEM- und EDR-Tools
- Automatische Verschlüsselung aller Daten im Ruhezustand
- Volle GDPR-Compliance
- Regelmäßige Vulnerabilitäts-/Penetrationstest
 - Schwachstellenanalysen sind automatisierte Tests zur Aufdeckung von Schwachstellen mithilfe eines automatisierten Tools, das alle externen Zugangspunkte scannt.
 - Bei Penetrationstests handelt es sich um autorisierte, simulierte Angriffe auf eine Automatisierungslösung, die von einem Team unabhängiger Sicherheitsexperten durchgeführt werden, um potenzielle Sicherheitslücken zu ermitteln, die ausgenutzt werden könnten, um Zugriff auf Funktionen und Daten zu erhalten.
- Alle Software- und Hardware-Anbieter sollten gründlich überprüft und kontinuierlich kontrolliert werden, um sicherzustellen, dass sie die Sicherheitsanforderungen erfüllen.
- Aktivitätsprotokolle gewährleisten die Verantwortlichkeit, helfen bei Prüfungsverfahren und liefern wertvolle Informationen, falls etwas schief geht.

2

Die Kommunikation und der Datenaustausch zwischen internen und externen Mitarbeitern werden verschlüsselt, um die Übertragung von Geschäftsdokumenten zu sichern, und alle eingehenden Dokumente werden systematisch auf Viren geprüft.

3

Richten Sie interne Zugangskontrollen ein und verwalten Sie diese selbst:

- Mehrere Ebenen der Authentifizierungssicherheit, die gewährleisten, dass nur befugtes Personal auf die Umgebung zugreifen kann.
 - Single-Sign-On-Verfahren (SSO), die die Sicherheit auf Benutzerebene erleichtern und zentralisieren.
 - Die Multi-Faktor-Authentifizierung (MFA) fügt der Plattformverbindung eine zusätzliche Sicherheitsebene hinzu, indem ein Token per E-Mail oder mobiler Anwendung versendet wird.
- Die Datentrennung durch eindeutige Dokumentenkennungen ermöglicht eine Zugriffskontrolle auf der Grundlage von vorgegebenen Berechtigungen.
- Eine breite Palette nachgelagerter Einstellungen wie die Definition von Benutzern, Profilen und Berechtigungen, die Kontrolle von Zugriff, Passwörtern und Sitzungsrichtlinien sowie die Einschränkung des Datenzugriffs, des Zugriffs auf IP-Adressen und der Sichtbarkeit von Dokumenten ermöglichen eine detaillierte Sicherheit und Transparenz der betrieblichen Aktivitäten.



...und zertifizieren

Diese Art von Sicherheitsmaßnahmen wird durch Zertifizierungen von Dritten sowie durch umfassende Schulungen für alle Mitarbeitenden des Unternehmens, die Zugang zu Daten haben oder mit ihnen umgehen, ergänzt. Eine Zertifizierung ist zwar keine Sicherheitskomponente an sich, aber sie kann bestätigen, dass diese Maßnahmen wirksam sind, und sie stellt sicher, dass alle Beteiligten auf dem gleichen Stand sind und immer auf dem neuesten Stand bleiben.

Einige wichtige Zertifizierungen sind:



ISO 27001

Diese Zertifizierung beinhaltet ein jährliches, gründliches Audit durch einen unabhängigen Prüfer, der die Wirksamkeit des Sicherheitsmanagements – wie Richtlinien und Verfahren – validiert und die kontinuierliche Verbesserung der Plattform gewährleistet.



SOC 1® Type 2 und SOC 2 Type 2 (SSAE 18 & ISAE 3402)

Diese Audits zertifizieren die Qualität und Integrität der internen Kontrollprozeduren.



HIPAA & HITECH

Diese Compliance-Protokolle bedeuten, dass sensible Gesundheits- und Patientendaten geschützt sind.

Infrastruktur: Cloud Computing öffnet den Himmel

Zuverlässigkeit, Monitoring, Skalierbarkeit & Redundanz

Cloud Computing bietet schnellere Innovation, flexible Ressourcen und Größenvorteile. Es senkt nicht nur die Kosten, sondern hält die Anwendungen auch auf dem neuesten Stand und bietet die Möglichkeit, Sicherheitsprotokolle zu integrieren, so dass Sie sich auf geschäftsrelevante Aufgaben konzentrieren können. Vor allem aber ist es viel einfacher, schnell und einfach zu skalieren: Ob 10 oder 10.000 Benutzer, Sie können sie mühelos bewältigen.

Um optimale Funktionalität zu gewährleisten, sollte eine Cloud-Computing-Struktur Folgendes bieten:



Zuverlässigkeit

Das Aufteilen von Daten in Datensätze sowie Redundanz- und Lastverteilungskonfigurationen auf mehrere Server verstärkt die Sicherheit, maximiert die Verarbeitungsgeschwindigkeit und gewährleistet die Servicekontinuität.



Monitoring

24/7-Überwachung gewährleistet die betriebliche Kontinuität mit mehreren Redundanzschichten, die mögliche Hardwareausfälle abfangen. Dies sorgt für eine hohe Serviceverfügbarkeit, und Probleme können leicht behoben werden, bevor sie den Endbenutzer beeinträchtigen. In Kombination mit Verfahren, die Risikomanagement, Incident Response, RTO/RPO umfassen, ermöglichen diese Systeme die Berechnung potenzieller Risiken und die Minimierung negativer Auswirkungen.



Skalierbarkeit

Anwendungen und Infrastrukturen müssen so entworfen und gebaut werden, dass sie sich leicht skalieren lassen, sowohl vertikal als auch horizontal. Die Nutzung einer Hyperscale-Architektur, die über verschiedene geografische Standorte verteilt ist und je nach Aktivität hoch- oder herunterskaliert

werden kann, garantiert Betriebszeit und hohe Leistung. Die Verarbeitungskapazität kann erhöht werden, ohne die aktuelle Produktion zu beeinträchtigen, und vertragliche Verpflichtungen bezüglich Lieferanforderungen werden effizient erfüllt.



Redundanz

Die Redundanz der Daten stellt sicher, dass, wenn ein Speicherort kompromittiert wird, die Wiederherstellung dennoch von den anderen Standorten möglich ist. Und es sind nicht nur die Daten, die redundant gemacht werden, sondern auch Server, Serverkonfigurationen, Datenbanken, Speicherorte, Dienste und mehr. Und obwohl „die Cloud“ selbst virtuell ist, hat sie auch eine sehr physische Dimension: Die Integrität und Sicherheit der Server muss jederzeit gewährleistet sein. Durch die Nutzung von Plattformen wie Microsoft Azure-Servern werden die Daten im Ruhezustand mit Azure Disk Encryption und basierend auf BitLocker und DM-Crypt verschlüsselt. Dies schützt die Daten sowohl vor Umwelt- als auch vor Zugriffsbedrohungen. Eine weit verbreitete physische Verteilung und Replikation, oft sogar innerhalb derselben Stadt, gewährleistet die Geschäftskontinuität, selbst wenn ein zerstörerisches Ereignis eintritt.



Dreifache Replikation von Daten gewährleistet Zuverlässigkeit

Lokal redundante Speicherung (Locally redundant storage, LRS)



Kopiert Daten synchron in drei Instanzen
in der primären Region.



Geo-Replizierung

Kopiert Daten asynchron offline in
drei Instanzen an einem sekundären
Standort, der geografisch weit von
der primären Region entfernt ist.

Agile Methodik

Ein weiterer Indikator dafür, wie gut die Lösung funktioniert, ist ihre Architektur. Obwohl es verschiedene Versionen der agilen Methodik gibt, hat sich der allgemeine Ansatz als effizienter und hochproduktiver Weg zur Softwareentwicklung erwiesen.



Um die sogenannte „konzeptionelle Integrität“ zu erreichen, müssen die User das Gefühl haben, dass die Lösung einfach zu bedienen ist, alle benötigten Funktionen hat und leicht gewartet, angepasst und skaliert werden kann. Das Gesamtbild während der inkrementellen und iterativen Entwicklung zu sehen, ermöglicht eine schnellere Entwicklungsgeschwindigkeit, Flexibilität und Produktivität.

Das vielleicht überzeugendste Argument für die agile Methodik ist die Reaktionsfähigkeit, die sie bietet. Die Fähigkeit, sich schnell an sich ändernde Bedürfnisse und Anforderungen anzupassen, anstatt eine Wasserfallmethodik zu verwenden, ermöglicht schnelle Anpassungen an sich ändernde Kundenbedürfnisse, Marktbedingungen und Bedrohungen durch Wettbewerber.

Die Schöpfer des agilen Ansatzes haben das Konzept so zusammengefasst:

- **Individuen und Interaktionen sind wichtiger als Prozesse und Tools**
- **Funktionsfähige Software ist wichtiger als umfassende Dokumentation**
- **Zusammenarbeit mit dem Kunden ist wichtiger als Vertragsverhandlung**
- **Reagieren auf Veränderungen ist wichtiger als die Befolgung eines Plans.**

agilemanifesto.org

Nahtlose Konnektivität

Integration, Integration, Integration

Heutzutage ist eine nahtlos verbundene IT-Landschaft ein absolutes Muss, um die Effizienz jeder Automatisierungslösung zu gewährleisten. Dies wird am besten durch bidirektionale programmgesteuerte Schnittstellen erreicht, die Ihnen helfen, eine einheitliche Sicht auf die Abläufe zu erhalten, Prozesse zu optimieren und einen konsistenten Datenfluss sicherzustellen.

Hier sind einige Funktionen, die den ununterbrochenen und reibungslosen Betrieb einer vielfältigen Systemlandschaft unterstützen:



Middleware & interne Applikationen

Middleware, Business- und IT-Applikationen leisten ihre Arbeit, indem sie eine Brücke bilden, die den Datenaustausch zwischen verschiedenen Anwendungen ermöglicht. Diese Konnektivität erlaubt es einer Automatisierungslösung, mit verschiedenen Systemen (ERPs, CRM usw.) zu interagieren, was eine einfache Bereitstellung und Einführung erleichtert. Sie garantiert auch Aufwärtskompatibilität und minimiert Implementierungskosten.



Robuste Integrationsmöglichkeiten

Ein breites Spektrum an Integrationsmöglichkeiten, einschließlich APIs und Webdiensten, ermöglicht Echtzeit-Datenmanagement, asynchrone Fehlerbehandlung und Unterstützung durch Third Party Monitoring. Unternehmen können Daten aus mehreren Systemen konsolidieren und gleichzeitig sicherstellen, dass die Informationen aktuell und genau sind. Die Unterstützung der Massenintegration mit Business-Intelligence- und

Process-Mining-Software ermöglicht zudem fundierte Entscheidungen auf Basis wichtiger Kennzahlen.



EDI & Managed File Transfer

Vor nicht allzu langer Zeit begann EDI als veraltete Methode des Dokumentenaustauschs zu gelten. Mit der Verbreitung von Gesetzen zu E-Rechnungsanforderungen in einer Vielzahl von Ländern auf der ganzen Welt fand EDI plötzlich wieder seine Daseinsberechtigung.

EDI bietet jetzt direkte Verbindungen zu B2G- und B2B-E-Rechnungsplattformen wie PEPPOL, Chorus Pro (Frankreich), FACe (Spanien) und SDI & NSO (Italien). Eine Vielzahl von Geschäftsdokumenten, wie Bestellungen, Bestellbestätigungen, Rechnungen und Bestandsberichte, können einfach und schnell verwaltet werden. Mit sicheren und zuverlässigen Kommunikationsmethoden wie AS2, SFTP und anderen Webdiensten werden mehrere EDI-Standards und -Formate (z. B. EDIFACT, X12, UBL und IDOC) unterstützt und verbinden die Systeme eines Unternehmens problemlos mit anderen Diensten, wodurch effiziente und zuverlässige Source-to-Pay (S2P)- und Order-to-Cash (O2C)-Prozesse entstehen.



Esker bietet eine einzigartige Lösung, die sowohl Rechnungen als auch Bestellungen verwaltet, was zu Effizienz in den Source-to-Pay- und Order-to-Cash-Prozessen führt.

Die Plattform von Esker wächst mit uns, passt sich unseren Bedürfnissen an und bietet uns eine sehr wettbewerbsfähige Gesamtkostenstruktur.

Gregor Miklavčič
European IT Manager, URSA

Mehr als Einzellösungen

Eine globale Plattform zum Schutz von Daten und zur Skalierung von Abläufen

Bei der Auswahl einer Automatisierungslösung muss das IT-Team die folgenden Schlüsselfaktoren berücksichtigen, damit das Unternehmen von optimierten Abläufen profitieren kann. Anstatt einer Mischung aus verschiedenen Einzellösungen bietet eine konsolidierte, globale Plattform für S2P- und O2C-Prozesse mehrere Vorteile:



Eine hollistische Automatisierung sorgt für Zuverlässigkeit

Die Einführung einer globalen Automatisierungsplattform beseitigt die Komplexität der Verwaltung mehrerer Systeme und stellt konsistente Prozesse sicher. Zuverlässigkeit ist in eine solche Struktur eingebaut, was Stabilität und Widerstandsfähigkeit bietet. Unternehmen können ihre Abläufe mit Zuversicht skalieren, ohne sich um Kompatibilitätsprobleme oder Systemausfälle sorgen zu müssen.



Datensicherheit & Compliance

Eine robuste Plattform sollte Daten- und Cybersicherheit priorisieren, da ein Unternehmen sensible Informationen schützen muss, während es die Branchenstandards einhält. Plattforminterne Sicherheitsmaßnahmen, einschließlich der Verschlüsselung eingehender und ausgehender Datenkommunikation, interner Zugriffskontrollen und Zertifizierungen, sind unerlässlich. Regelmäßige Sicherheitsschulungen stellen sicher, dass die Mitarbeitenden ihre Rolle bei der Aufrechterhaltung einer sicheren Umgebung verstehen



Monitoring, Transparenz & Skalierbarkeit

Echtzeit-Überwachungsfunktionen bieten Einblick in ihre Prozesse, um Engpässe zu identifizieren und Arbeitsabläufe zu optimieren. Skalierbarkeit stellt sicher, dass die Lösung mit dem Unternehmen wachsen kann. Darüber hinaus ermöglicht Transparenz den Stakeholdern, Leistungskennzahlen zu verfolgen und fundierte Entscheidungen zu treffen.



Nahtlose Integration mit Middleware, Business-Apps & ERPs

Konnektivität ist entscheidend, und eine Automatisierungsplattform sollte sowohl sofort einsatzbereite Konnektoren zu verschiedenen Anwendungen über sichere APIs und Webdienste bereitstellen. Je mehr eine Automatisierungslösung Flexibilität und Anpassungsfähigkeit bietet, desto reibungsloser verlaufen die Abläufe und desto weniger müssen Sie sich mit Interoperabilitätsproblemen auseinandersetzen.

Indem eine umfassende Plattform priorisiert wird, die Automatisierung, Sicherheit, Skalierbarkeit, Konnektivität und Transparenz kombiniert, können der CIO und sein Team dem Unternehmen optimierte Prozesse, Datenintegrität und effiziente Zusammenarbeit in den S2P- und O2C-Funktionen bieten.

Hi, wir sind Esker

Eskers KI-Automatisierungssuite für das Office of the CFO nutzt die neuesten Technologien im Bereich Agentic AI und Automatisierung, um das Working Capital und den Cashflow zu optimieren. Zugleich werden strategische Entscheidungen verbessert und die zwischenmenschlichen Beziehungen zu Kunden, Lieferanten und Mitarbeitenden gestärkt. Eskers Lösungen für Source-to-Pay und Order-to-Cash automatisieren diese Geschäftsprozesse und unterstützen gleichzeitig langfristige Wachstumsstrategien.



> 40

Jahre Erfahrung, davon mehr als 20 Jahre in der Cloud



> 1.200

Mitarbeitende betreuen mehr als 1.120.000 User und 3.000 Kunden weltweit



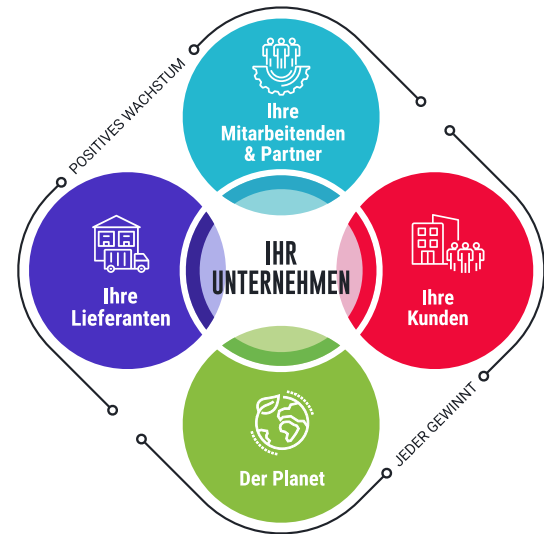
15

globale Standorte mit Hauptsitz in Lyon, Frankreich, & zwei deutschen Niederlassungen



~250 Mio. €

Umsatz im Jahr 2025



Erfolg ist am besten, wenn man ihn teilt

Wir bei Esker glauben, dass der einzige Weg zu einer echten, sinnvollen Veränderung in einem positiven Wachstum (wir nennen es Positive Sum Growth) besteht. Das bedeutet, dass der Geschäftserfolg nicht auf Kosten eines Einzelnen, einer Abteilung oder eines Unternehmens geht – alle gewinnen! Aus diesem Grund ist unsere KI-gesteuerte Technologie so konzipiert, dass sie alle Stakeholder unterstützt und gleichzeitig eine langfristige Wertschöpfung fördert.



ESKER®
www.esker.de

©2020 Esker S.A. All rights reserved. Esker and the Esker logo are trademarks or registered trademarks of Esker S.A. in the U.S. and other countries. All other trademarks are the property of their respective owners.