SICHERHEIT IM AGILEN VORGE-HEN

Daniel Augustin, Geschäftsführer, SSE Secure Systems Engineering
Dr. Waldemar Grudzien, Expert Director, CORE SE

30.10.2018
COREtechmonitor | Blogpost

Key Facts

- Agile Entwicklung „übersieht“ ganzheitliche Sicherheitsanforderungen
- Security Ambasador verbindet agiles Entwicklungsvorgehen mit gebotener ganzheitlicher Sicht auf Sicherheit
- Messbare Sicherheitseigenschaften werden Qualitätsmerkmal wie Produkt-Features
- Security-by-Design ist kein Code-freeze, muss vielmehr in jedem Sprint neu hinterfragt werden
- Umsichtige Sicherheitsplanung bereitet intrinsisch Auditierung vor

Der Wandel von Software- und Infrastrukturprojekten

Software- und Infrastrukturprojekte unterliegen einem grundlegenden Wandel. Der Trend liegt heute bei kleinen agilen Teams, die unabhängig voneinander und nicht selten räumlich getrennt voneinander arbeiten. Sie entwickeln abgeschlossene Teilprogramme, die über abgestimmte Schnittstellen miteinander kommunizieren und so ein Gesamtsystem bilden. Das agile Vorgehen bringt grundlegende Vorteile mit sich, die besonders in komplexen Projekten zum Tragen kommen. So entwickeln kleine Teams produktiver, denn sie harmonieren besser miteinander, wählen ihre eigenen Methoden und Werkzeuge und folgen ihrem eigenen Rhythmus. Auch bietet die Trennung organischer Systeme in unabhängige Teilkomponenten einen spürbaren Mehrwert hinsichtlich Wartbarkeit und Beurteilungsfähigkeit. Die IT-Sicherheit darf diesen Umstand nicht durchbrechen, sondern muss ihn für sich nutzen.

Im direkten Vergleich eilt die Evolution der Softwareentwicklung der der IT-Security voraus, die zu großen Teilen noch immer im Wasserfallmodell agiert. Dieser Umstand ist nicht unbegründet, denn für eine Sicherheitsbetrachtung ist die ganzheitliche Sicht auf das Produkt erforderlich. Sicherheitsexperten gruppieren Daten in Schutzbedarfsklassen, die sich aus Schutzzielen (z.B. Datenschutz, Zertifizierbarkeit, Produktphilosophie) der zu schützenden Informationen ableiten, und betrachten dann all jene Komponenten und Verbindungswege, die mit ihnen wechselwirken. Verwundbarkeiten und sich daraus ableitende Angriffsformen resultieren in technischen, organisatorischen und personellen Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit und Schadenshöhe. Eine Sicherheitsbetrachtung findet auf allen Ebenen eines Software- und Infrastrukturprojekts statt und steht daher scheinbar im Widerspruch zu agilen Projektstrukturen.

Projektkosten, verbleibendes Restrisiko und Aufwand für Umsetzbarkeit steigen, je später mit der Umsetzung geeigneter Maßnahmen begonnen wird. Die besten Ergebnisse werden unserer Erfahrung nach mit einer Ergänzung des agilen Modells um die Funktion des „Security Ambassadors“ erzielt.

Security Ambassador als Botschafter zwischen den Welten

Die Harmonisierung agiler Projekte mit einer eher monolithischen Sicherheitsbegleitung ist eine spannende Herausforderung. Das Ziel ist nicht weniger als die Verknüpfung zweier Welten, die kaum unterschiedlicher sein könnten. Die kompromisslose Koexistenz zwischen Wasserfall und Agilität führt unweigerlich zu Frust. Sicherheitsexperten fühlen sich nicht ernst genommen und Entwickler bevormundet und ausgebremst. Die

Kommunikation wird schlechter und die Arbeit am Produkt als gemeinsamen Ziel gerät aus dem Fokus.

Dabei liegt die Lösung auf der Hand. Zur Herstellung einer Resonanz müssen Sicherheits-experten zu Teammitgliedern werden. Sogenannte Security Ambassadors fungieren als Adapter zwischen beiden Welten. Sie verfügen über Sicherheitsexpertise, wenden diese jedoch ausschließlich in den Grenzen des einen agilen Teams an, dem sie zugewiesen wurden. Mit dem Wissen über systemübergreifende Sicherheitszusammenhänge stehen sie beratend zur Seite, erarbeiten Vorgehensmodelle und begleiten sicherheitsrelevante Userstories. Als Botschafter führen sie die Kommunikation mit der übergeordneten Sicherheitsinstanz und bringen ihre Erkenntnisse in die Gesamtsicherheitsbetrachtung ein. Umgekehrt können Sicherheitsambassadoren jederzeit auf die Expertise und Zuarbeit der Security Ambassadoren aus anderen Teams und ggf. den Sicherheitsexperten der Projekt owner zurückgreifen.

Entwicklung fokussiert auf Features

IT-Sicherheit und Datensicherheit sind notwendige Voraussetzungen für die erfolgreiche Digitalisierung von Geschäftsprozessen. Sie schaffen Vertrauen bei Kunden, Partnern, der Öffentlichkeit und nicht zuletzt bei Aufsichtsbehörden durch wirksamen Schutz vor wirtschaftlichen und Schäden der Reputation. Die Notwendigkeit einer funktionierenden IT-Sicherheit steht außer Frage und wird erfahrungsgemäß auch nicht angezweifelt. Dennoch hakt es häufig bei ihrer Umsetzung.

Einen Grund hierfür findet man in der betriebswirtschaftlichen Betrachtung. IT-Sicherheit dient in erster Linie der Vermeidung von finanziellen Schäden und der Reputation. Sie kostet Geld anstatt es zu verdienen. Stellt man folglich Investition und Ertrag gegenüber, schneiden sichere Lösungen grundsätzlich schlechter ab – solange nichts passiert.

Mit funktionalen Anforderungen – den Features – verhält es sich anders. Sie sind greifbar und führen zu Erträgen. Das liegt auch daran, dass sie vom Kunden als Qualitätsmerkmal verstanden und bei der Entscheidungsfindung zwischen sonst gleichwertigen Produkten herangezogen werden. Sicherheit ist aus der Perspektive eines Kunden ein schwer messbares und inflationär eingesetztes Werbeversprechen. Auch in der Softwareentwicklung spiegelt sich dieser Umstand wider. In den einzelnen Phasen eines Projekts präsentieren die agilen Teams ihre Deliverables, d.h. funktionsfähige Zwischenlösungen. Ihre Bewertung durch Stakeholder erfolgt anhand greifbarer Marker. Das sind in der Regel Features. Dabei besteht kein Grund dafür, dass die IT-Sicherheit als nichtfunktionale Anforderung hier ein Schattendasein fristet. Sie kann ebenfalls als greifbarer Fortschritt kommuniziert werden. Penetrationstests ohne auffällige Befunde sind hier nur eine Möglichkeit. Auch Linting-Werkzeuge mit Security-Audit-Regeln oder frei verfügbare Online-Analysewerkzeuge können Lösungen und Zwischenlösungen ein hohes Sicherheitsniveau bescheinigen. Zertifizierte IT-Sicherheit ist ein messbares Qualitätsmerkmal, das sich nach außen transportieren und als Produktmerkmal monetarisieren lässt.

Die Voraussetzungen hierfür sind denkbar einfach: Sowohl die Projektleitung als auch die Geschäftsführung müssen sich klar zur Sicherheit bekennen und diese bei Anforderungsspezifikationen und Abnahmen gleichwertig zu Features behandeln.

Transfer von Sicherheitswissen in agile Systeme

Betrachtet man die OWASP-Liste der häufigsten Schwachstellen und erfolgreichsten Angriffe, so entdeckt man seit Jahren stabile Verhältnisse. Die gängigsten Angriffe wie Injection, Bruteforce und die üblichen Schwachstellen wie Fehlkonfigurationen, fehlendes Schwachstellen-/ Patchmanagement, unzureichendes Monitoring oder mangelhafte Zugriffskontrollen halten sich seit 2010 beharrlich an der Spitze der Charts.

Für die meisten der Verwundbarkeiten existieren Hilfsmittel zur Identifizierung und Bewertung. Sie kommen bei Penetrationstests zum Einsatz. Aufgedeckte Lücken lassen sich so durch Entwickler oft ohne Zuhilfenahme von Sicherheitsexperten schließen. Beobachtungen in Großprojekten haben jedoch gezeigt, dass sich einst geschlossene Sicherheitslücken in späteren Projektphasen nicht selten wieder öffnen.

Eine agilere Sicherheitsbetreuung bietet hier Abhilfe. Über Linting-Werkzeuge innerhalb der kontinuierlichen Integration (CI) findet ein Transfer von Wissen um gängige Schwachstellen statt. Bekannte Schwachstellen und Lösungshinweise können dadurch eigenständig und ohne Zutun von Sicherheitsexperten abgerufen und Korrekturen umgesetzt werden. Die Frequenz erforderlicher Penetrationstests sowie der Aufwand interner Audits verringern sich, was zu einer deutlichen Beschleunigung des Entwicklungsprozesses führt.

Deckt man die gängigsten Bedrohungen automatisiert ab, dann kann man sich den individuellen und technologie-, regulatorisch- oder branchenspezifischen IT-Sicherheitsherausforderungen widmen. Denn durch diese Treiber entstehen permanent neue Angriffsvektoren und neue Schwachstellen bedingt durch die Komplexitätszunahme eines Ökosystems, das in Bestandteile aufgebrochen und auf mehrere Player aufgeteilt wird – einfaches Beispiel: Online-Zahlungssysteme und Markteintritt Dritter bedingt durch die PSD II.

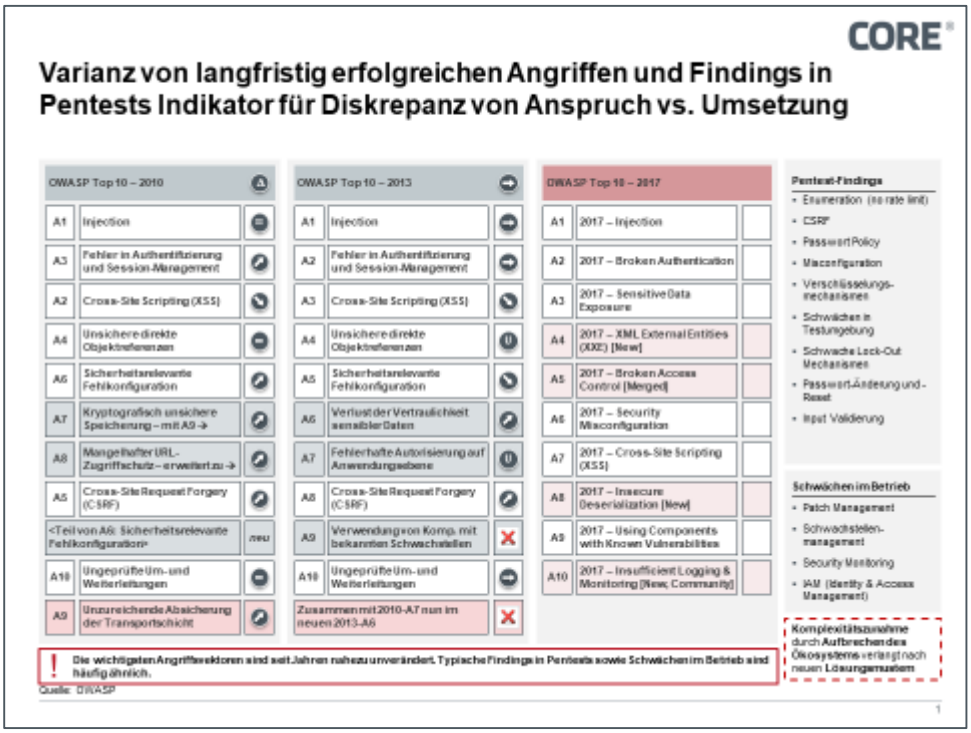

Abbildung 1: Erfolgreiche Angriffe, Pentest Findings und Schwächen in Operations zeigen langjähriges stabiles Verhalten

Buzzword Security-by-Design

Security-by-Design schreiben sich alle auf die Fahne, nicht zuletzt weil es Regulierung und Aufsicht kodifiziert haben. Jedoch bleibt ab dem Start davon oft nicht mehr viel übrig. Systemdesign und Architekturentwurf tendieren aufgrund zunehmender Anforderungen zu einem „ball of mud“, in dem alles noch irgendwie hineinimplementiert wird, um den nächsten Sprint, das nächste Release, einzuhalten. Sicherheitsbelange, Dokumentation und Review des Codes kommen oft zu kurz. Sicherheit als nichtfunktionales Thema wird häufig nur temporär und zusätzlich erst später im fortgeschrittenen Projekt involviert, dann soll ein Design „schnell sicher gemacht werden“, denn Sicherheit „erzeugt nur Aufwände und verdient kein Geld“. Sicherheit wird als Blocker der Feature-Entwicklung wahrgenommen und folglich häufig entsprechend minder priorisiert.

Die Eigenheiten moderner Softwareentwicklung bedingen weitere Herausforderungen, die sich erschwerend auf die angemessene Einbindung von Sicherheitsaspekten auswirken. Heutzutage bestehen Projekte oft aus global verteilten Entwicklungsteams. Sie sind räumlich auf Länder und Zeitzonen verteilt, ihre Mitglieder sprechen verschiedene Sprachen. Doch nicht nur die Entwickler haben keine gemeinsame Lingua franca, auch die einzelnen Domänenmitglieder sprechen verschiedene „Sprachen“ wie Business, Marketing, Legal, Sicherheit usw. Beide Sprachphänomene führen zu Verständigungsproblemen, die letztendlich zu „missverstandenem“, intrinsisch unsicherem Code führen. Die räumliche,

zeitliche und sprachliche Verteilung sowie das Zeitkorsett des agilen Vorgehens erfordern eng getaktete Absprachen die diszipliniert eingehalten werden müssen. Droht ein Riss im Zeitplan, bleiben zuerst die nicht-funktionalen Anforderungen auf der Strecke. Ziel muss die Änderung der Operationalisierung der Entwicklung durch Verbindung von Coden und Security sein.

Security-by-Design beginnt mit den richtigen Fragen

Die Sicherheit eines Systems ist kein Codefreeze, sondern ein agiler Prozess, in dem durch kontinuierliche Hinterfragung der wesentlichen 5 Systemvariablen eine ganzheitliche Sicht auf die Systemsicherheit erreicht wird:

- **Modell:** Welche Außenschnittstellen werden zur Verfügung gestellt? Wird auf eine dedizierte oder eine cloudbasierte Infrastruktur gesetzt? Handelt es sich um eine verteilte oder eine zentralisierte Lösung? Wie erfolgt der Domänenzuschnitt auf Microservices? Liegt die Präferenz auf Eventsourcing oder Datenbanken? Das Systemmodell bestimmt maßgeblich die möglichen
- **Angriffe/ Schwachstellen:** Wie schütze ich Eingaben in mein System? Welchen Einfluss habe ich auf die Sicherheit der von mir eingesetzten Werkzeuge, Bibliotheken und Services? Wie verhindere ich Enumeration-, Bruteforce- oder Fingerprinting-Attacks durch die ungewollte Preisgabe von Systeminterna? Besteht eine Bedrohung durch Innentäter oder Priviledge Eskalation Angriffe? Die identifizierten möglichen Angriffe und Schwachstellen erfordern passgenaue
- **Maßnahmen:** Welche technischen, organisatorischen oder personellen Maßnahmen führen zu einer Reduzierung der Eintrittswahrscheinlichkeit von Angriffen (z.B. Eingabevalidierung, Vulnerability und Patchmanagement oder Härtung von Komponenten, Netzwerkzonen)? Existieren zusätzliche Möglichkeiten zur Verringerung der Schadenshöhe durch Angriffe (z.B. Security Monitoring, Incident Management, Hardware-Sicherheitsmodule)? Auf welche Weise lässt sich meine Organisation vor Innentätern (z.B. IAM, Seggregation of Duties, Sicherheitsschulungen) schützen? Verfüge ich über ein Zugriffsmanagement und Segregation of duties in Kernprozessen? Die Freiheitsgrade dieser Maßnahmen werden maßgeblich bestimmt durch die verwendeten
- **Technologien:** Neue Technologien müssen beherrscht werden, denn schlecht implementierte Technologien sind gefährlich. Das gilt für die gesamte Toolchain, verwendete Protokolle wie OAUTH 2.0 und OpenID Connect und selbstverständlich auch für die richtige Parametersetzung in Bibliotheken und Frameworks. Über allem schweben
- **Regulierung/ Aufsicht:** Welche Regulierungen und Aufsichtsregime bestimmen wie mein Systemmodell und die gewählten Technologien und Maßnahmen? Cloud oder Nicht-Cloud? Nur innerhalb der EU? US-Homeland Security Act? Welche personenbezogenen Daten werden wo verarbeitet? Kann

mein System einzelne Datenfelder löschen? Auch in Backups und Archiven?

Fragen über Fragen, die von Anfang an konzentrierte und fokussierte Experten der sicheren agilen Entwicklung bedürfen.

Lessons learned

Zur Verbesserung der Integration von Features und Security bieten sich einige in Projekten diverser Größe gemachte Lessons learned an. Diese Erfahrungen sind eigentlich auf der Hand liegende einfache, in der Praxis jedoch nicht als Selbstläufer umsetzbare Maßnahmen. Sicherheit in der agilen Entwicklung ist eine Teamleistung – so einfach, so schwierig. Im besten Fall sollten alle Entwicklungsteams zur gleichen Zeit am gleichen Ort am Projekt arbeiten. Die gleiche Sprache bietet einen großen Vorteil. Im zweitbesten Fall arbeiten die verschiedenen Domänenteams verteilt am Projekt. Team Domäne 1 am Ort 1, Team Domäne 2 am Ort 2 usw. Entscheidend ist die Zugehörigkeit des Security Ambassadors zu seinem Team. Dieser muss im Team ein gleichberechtigtes Mitglied sein.

Denn in Anlehnung an das Extreme Programming hat sich die enge Begleitung der Entwickler durch die neu installierte Funktion des Security Ambassadors pro Business-Domäne gut bewährt. Der Security Ambassador fungiert als Berater der Entwickler, der Probleme mit löst und nicht nur Forderungen stellt und auf die Erledigung wartet. Dieses Vorgehensmodell bedeutet tägliche harte Kümmerarbeit und belohnt mit sicheren Systemen. Bei länger laufenden Projekten kann eine Teamrotation des Security Ambassadors nach einigen Monaten erwogen werden, um einem „Kumpaneieffekt“ mit Nachsichteffekten vorzubeugen.

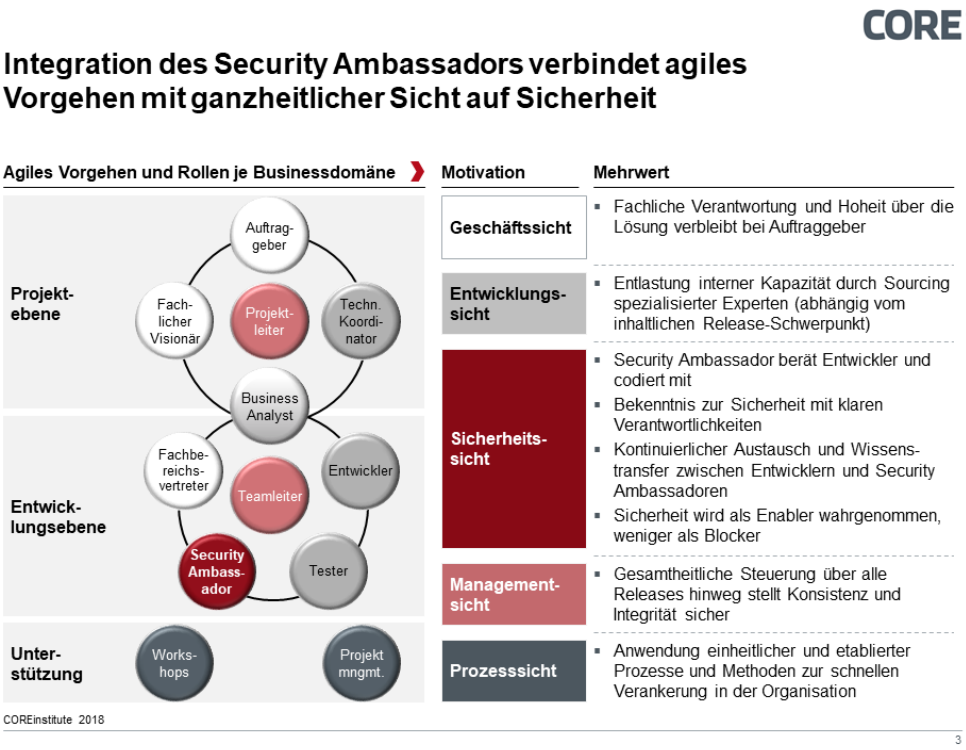

Abbildung 2: Security Ambassador verbindet Vorteile des agilen Entwicklungsmodells mit der gebotenen Präzision für Sicherheitsanforderungen des Wasserfall-Modells

Durch Integration von Codeanalysetools und eigen entwickelter Sensorik in die Deployment-Kette werden Entwickler im besten Falle in die Lage versetzt, bereits in ihrer Entwicklungsarbeit sicherheitskritische Codeelemente zu erkennen und in Zusammenarbeit mit dem Security Ambassador zu heilen.

Wird Security-by-Design von Anfang an im Projekt berücksichtigt, findet eine Verantwortungsverlagerung für Sicherheit in das Architektur- und Produktdesign statt. In der Designphase werden Assets und Schutzziele aus (abstrakten) Anforderungen der Produktphilosophie (User Experience, Datenschutz, Zertifizierbarkeit, ...) abgeleitet und durch Aufteilung großer Aufgaben in mehrere kleine Aufgaben (Segregations of concerns) wird „nebenbei“ auch die Beurteilungsfähigkeit des Systems vorbereitet. Maßnahmen „from the scratch“ werden als Teil der Architektur (z.B. Encryption service) eingeplant und ermöglichen eine flexible Gestaltung der Security für zukünftige Änderungen („Kryptoagilität“). Zwischen Entwicklern und Security Ambassadoren findet ein kontinuierlicher Austausch und Wissenstransfer statt, die Sicherheit wird so mehr als Enabler (Features, Usability, ...) und weniger als Blocker wahrgenommen.

In der Implementierung müssen im Projektmanagement wenige Institutionen und Verantwortliche beteiligt sein, die mit klarer Zuweisung für Verantwortlichkeiten und Prozessabläufe die Akzeptanz der Sicherheit als weiteres und gleichberechtigtes Designziel vom Team durch eigenes positives Tun erhöhen. Die Security Ambassadoren wer-

den in ihren Domänen in Entscheidungsprozesse integriert. Dadurch wird im Projekt ein Bekenntnis zur Sicherheit mit klaren Verantwortlichkeiten verankert.

Fazit

Seit Dekaden wird versucht Sicherheit und Features zu versöhnen. Ein Schritt auf diesem Wege ist aus unserer Sicht die Integration der Funktion Security Ambassador in die agilen Entwicklungsteams. Dieser arbeitet ab Sprint Null gleichberechtigt zu den funktionalen Anforderungen am Produktziel mit und fungiert nach außen gesamtverantwortlich für die Produktsicherheit. Diese Ergänzung des agilen Modells verbindet agiles Vorgehen mit ganzheitlicher Sicht auf Sicherheit, die auf Erfahrungen unserer Projekte der letzten Jahre baut. Durch das konsequente Behandeln der Sicherheitsanforderungen als gleichberechtigte Zielmarken wird die Sicherheit eines Systems beurteilungsfähig, ergo zertifizierbar; eine mittlerweile geforderte Eigenschaft der Aufsicht. Insgesamt wird IT-Sicherheit zu einem messbaren Qualitätsmerkmal wie funktionale Produkt-Features, das sich nach außen transportieren und als Produktmerkmal monetarisieren lässt.

Sources

The Open Web Application Security Project (OWASP): https://www.owasp.org/index.php/Main_Page

Dr. Waldemar Grudzien setzt sich als Expert Director mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@core.se

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
P.O. Box 506656 Dubai I UAE
https://www.core.se
office@coretransform.ae