WHITEPAPER

Cyber Security
im Fokus der CxOs: Die Herausforderungen an Unternehmen wachsen

Learn more at tispayments.com »

EXECUTIVE BRIEFING

Mit *Cyber Security* findet sich ein neues, zentrales Thema auf der Agenda von CxOs: direkt als Top Zwei hinter *Digital Transformation*, wie die Management-Beratung Horváth in der aktuellen Ausgabe ihrer jährlich erstellten CxO-Studie von Juni 2022 jüngst herausgefunden hat.. Während Unternehmen aus der Finanzbranche und Versicherungen bereits länger mit dem Thema konfrontiert und besser darauf vorbereitet sind, gilt es nun insbesondere für produzierende Unternehmen, Lösungen für resiliente, sichere und skalierbare Prozesse zu finden. TIS bietet mit **RiskOptix** ein breites Portfolio innovativer Technologien, um mit digitalen Mitteln diese Herausforderungen zu meistern.

VON NULL AUF PLATZ ZWEI.

Cyber Security ist der starke Neueinsteiger auf der Agenda des C-Levels in 2022

Die digitale Transformation ist für Unternehmen verschiedenster Größen und Branchen ein Thema, das nicht zuletzt durch die Pandemie deutlich an Fahrt gewonnen hat. In den Bereichen Finanzen, Treasury und Accounting etwa werden von der Erstellung und Freigabe von Transaktionen bis hin zu deren Ausführung und Auswertung heute verschiedenste digitale Lösungen, neue Kanäle und Workflows genutzt, die teils als strategisches Instrument im Rahmen bereits angestoßener Digitalisierungsprozesse in den Unternehmen selbst implementiert worden waren, teils jedoch schlicht der rapiden Umstellung auf Home-Office-Situationen und mobiles Arbeiten geschuldet sind. Entsprechend der extrem kurzen Implementierungszeit weisen letztere oft Lücken und Schwachstellen auf, die Unternehmen potentiell besonders verletzlich für digitale Angriffe auf den Zahlungsverkehr machen.

Doch dies allein kann nicht hinreichend das überraschende Ergebnis der aktuell umgesetzten CxO-Studie von Horváth erklären, in der *Cyber Security* als neues, virulentes Thema fürs C-Level von Null direkt auf Platz Zwei katapultiert wurde.[1]

Die Managment-Beratung Horváth hat dieses Jahr mit 280 CxOs aus 17 verschiedenen Ländern, vor allem aus der EMEA-Region, intensive Gespräche zum Thema strategische Prioritäten und Branchentrends geführt:

General Study Information

- **280** CxOs im Gespräch mit Horváth
- **41%** CEOs - Spitzenmanager mit strategischem Weitblick
- **~200Std** Persönliche Gespräche mit top Entscheidungsträgern
- **13** Strategische Prioritäten für mittel-und langfristigen Unternehmenserfolg
- **13** Wochen mit Gesprächen zwischen dem 21. März und dem 17. Juni 2022
- **>240** Umsatzprognosen
- **10** Branchen berichten über Branchentrends
- CxOs aus 17 verschiedenen Ländern

Quelle: Horváth, CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, S. 4

1 Horváth: CxO Priorities 2022. Managing Overlapping Crises, Juni 2022.

VON EINER KRISE IN DIE NÄCHSTE:

Die Herausforderungen an Unternehmen wachsen

Für die neue Präsenz des Themas *Cyber Security* auf der Agenda der CxOs lässt sich ursächlich die aktuelle globalpolitische Lage heranziehen – stellt diese doch keine Entspannung in Aussicht. Neben nach wie vor bestehenden Lieferkettenengpässen und -verzögerungen verursachen die volatilen Märkte und politischen Instabilitäten auf globaler Skala massive Unsicherheiten. Sorge vor und Risiko von digitalen Attacken steigen deutlich,[2] während die sich ständig ändernden Sanktionen und Sanktionslisten zusätzliche Compliance-Herausforderungen für Unternehmen mit sich bringen.

Strategische Prioritäten in 2022 für mittel-und langfristiges Wachstum

	Rang 2020	Rang 2021	Rang 2022	△ '21 vs. '22	Score 2020	Score 2021	Score 2022
Digital Transformation	1	1	1	=	3.6	3.6	3.6
Cyber Security			2	NEU			NEU 3.5

Quelle: Ergebnis der Studie: Horváth: CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, S. 18

Während Banken, Versicherungen und Finanzdienstleister bereits seit einigen Jahren verstärkt mit dem Thema *Cyber Security* konfrontiert sind und entsprechende Maßnahmen implementiert oder zumindest evaluiert haben, sind es nun insbesondere produzierende Unternehmen, die sich neuen Herausforderungen gegenübersehen.

Cyber Security – der Rising Star 2022

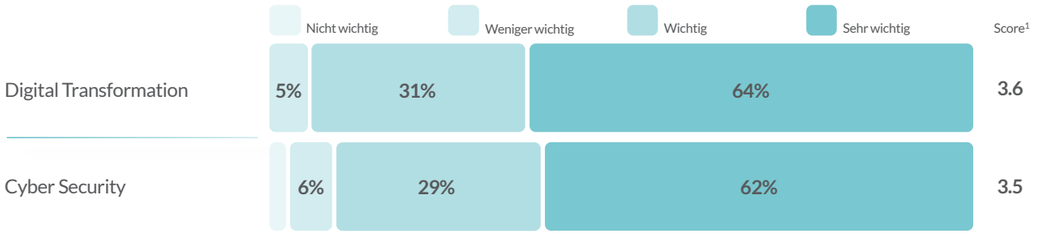
- Strategisches Kernthema zur Sicherung des operativen Geschäfts
- Strategische Priorität zur kurz- und langfristigen Sicherung des Wachstums
- Branchenüber-greifend an zweiter Stelle auf der Agenda der CxOs
- Top 1 Priorität für produzierende Unternehmen

Quelle: Horváth, CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, S. 4

2 Siehe Horváth: CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, S.18

91% der von Horváth befragten 280 CxOs betrachten das Thema *Cyber Security* als wichtig bzw. sehr wichtig. Der Abstand zum Spitzenreiter *Digital Transformation* – von 95 Prozent der Befragten als wichtig bzw. sehr wichtig eingeschätzt und unverändert wie 2020 und 2021 schon auf Platz Eins der Prioritätenliste von CxOs – ist gering.

Top Prioritäten: *Cyber Security* dicht hinter *Digital Transformation*



¹ *Wichtigkeit der Prioritäten auf einer Skala von 1-4: 4 - sehr wichtig, 3 - wichtig, 2 - weniger wichtig, 1 - nicht wichtig, 0 - nicht zutreffend*
Quelle: Horváth, CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, S. 17

RISIKEN KONSEQUENT MINIMIEREN
Mit den richtigen digitalen Lösungen

Cyber Security und *Digital Transformation* führen deutlich die strategische Agenda der CxOs in 2022 an. Und so ist es durchaus als Vorteil zu betrachten, dass sich beide Top-Themen mit den gleichen Werkzeugen und Strategien adressieren lassen und sich sogar teilweise in Wechselwirkung optimieren:

„Im Rahmen unserer Beratungstätigkeit im Treasury-Umfeld achten wir auf einen klaren organisatorischen Aufbau und integrierte Prozesse mit einem hohen Standardisierungs- und Harmonisierungsgrad. Dies gilt insbesondere bei einem so sensiblen Thema wie dem Zahlungsverkehr. Wir sehen hier auf unseren Projekten ein deutliches Potential an Transparenz- und Effizienzsteigerung.

Bei der Umsetzung von Digitalisierungsstrategien sind die Unternehmen auf der Suche nach geeigneten technischen Lösungen für die Abwicklung des Zahlungsverkehrs und stellen neben den typischen Anforderungen, wie Prozessunterstützung, Automatisierung und Monitoring vermehrt Anforderungen, die auf Flexibilität und Absicherung des Zahlungsverkehrs abzielen. Dies wird durch die Ergebnisse unserer CxO-Studie aus diesem Jahr unterstrichen. Wir gehen davon aus, dass sich dieser Trend in Zukunft fortsetzen wird."

Marco Meyer, Principal Treasury bei Horváth

Für *Cyber Security* im Allgemeinen und den Zahlungsverkehr im Besonderen heißt das etwa: mit Hilfe innovativer und sicherer digitaler Lösungen resiliente und belastbare Prozesse zu etablieren. Dies findet nicht nur punktuell statt, sondern harmonisiert auf globalem Level und entitätsübergreifend. Eine gesamtheitlich optimierte Standardisierung und Automatisierung der Prozesse, Systemzugänge und Verfügungsberechtigungen, wie etwa ein konsequentes n-Augen-Prinzip oder IP-Blocklists und -Whitelists, kann wesentlichen Anteil an dem erfolgreichen Agieren eines Unternehmens haben und dessen Resilienz in Krisenzeiten festigen.

Doch mit der Sicherung dieser grundlegenden Prozesse und Abläufe ist nur der erste Schritt getan. Da sich digitale Bedrohungen permanent weiterentwickeln und neue Betrugsszenarien entstehen, lässt sich diesen am besten mit digitalen Lösungen begegnen, die ebenso beständig und innovativ weiterentwickelt werden und über ein breites Grundinstrumentarium gegen sowohl interne als auch externe Sicherheitsbedrohungen verfügen. Sie müssen zudem die nötige Flexibilität mit sich bringen, um organisches und anorganisches Unternehmenswachstum ohne langwierige Implementierungsprozesse zeiteffizient und zukunftsorientiert unterstützen zu können.

SANCTION SCREENING & PAYEE COMMUNITY SCREENING:
Zentrale Funktionen in TIS RiskOptix

TIS verfügt als Cloud-basierte Lösung mit hoher Banken- und ERP-Konnektivität über die nötige Flexibilität und Skalierbarkeit, um in kurzer Zeit neue Unternehmensentitäten weltweit andocken zu können. Während die **RiskOptix**-Produktpalette standardmäßig bereits verschiedene wesentliche Sicherheitsfunktionalitäten, etwa automatisierte Workflows, sichere Logins, klare Rollen- und Rechteverteilungen sowie Datensicherheit und -verschlüsselung auf ISO 27001 und SOC1&2 zertifizierten Servern umfasst, sind es insbesondere zwei neuere Lösungen in RiskOptix, die sich vor dem Hintergrund der aktuellen globalpolitischen Herausforderungen als besonders wertvoll für Unternehmen erweisen können: das **Sanction Screening** & das **Payee Community Screening**.

Der Verstoß gegen Sanktionslisten kann nicht nur empfindliche Geldstrafen, sondern auch langfristige Rufschädigung nach sich ziehen, sodass sich aus einem Fehler im Zahlungsverkehr potenziell existenzgefährdende Situationen für ein Unternehmen ergeben können. Dem gegenüber stellen Umfang sanktionierter Länder, Parteien und Individuen – allein die OFAC listet mehr als 11.000 Einträge – und Geschwindigkeit sich ändernder Sanktionsvorgaben eine Herausforderung dar.

Einzelne Banken und Back-Office-Systeme wie Treasury Management Systeme (TMS) bieten das Screening von Zahlungen gegen Sanktionslisten an, doch Compliance auf globalem Level und für die Gesamtheit des Zahlungsverkehrs in sämtlichen Unternehmenssitzen ist hier aufgrund fehlender Konnektivität zu anderen Systemen, Banken und Entitäten zum Teil nicht gegeben. Automatisierung und weltweite Harmonisierung des Sanktionslistenscreenings als fester Bestandteil der gesamten Unternehmenszahlungen ist hingegen etwas, das TIS durch seine umfassende Systemkonnektivität beispielsweise anbietet. Täglich aktualisierte Sanktionslisten, etwa die der UN, EU und OFAC, lassen sich mit individualisierbaren Blocklists oder auch Whitelists ergänzen, sodass alle Zahlungen rund um die Uhr auf Basis der aktuellen Vorgaben geprüft werden können. Das Alert Management erfolgt global einheitlich, wird lückenlos dokumentiert und Verdachtsfälle werden mit klar definierbaren Verantwortlichkeiten gelöst – um maximale Compliance nicht nur bei den Zahlungen selbst, sondern auch bei der Bearbeitung von Verdachtsfällen zu ermöglichen.

> „Risiken und Schwachstellen im Zahlungsprozess entstehen häufig durch ungenügenden Datenaustausch zwischen Systemen in den unterschiedlichen Unternehmensentitäten. Bei so sensiblen Themen wie digitaler Sicherheit und der Einhaltung von Sanktionsvorgaben können sich aus diesen Lücken schwerwiegende Folgen für ein Unternehmen ergeben. TIS unterstützt durch die Kombination von automatisierten Prozessen mit digitalen Lösungen maßgeblich bei der weltweiten Einhaltung von Compliance-Vorgaben. Gleichzeitig werden im gesamten Zahlungsprozess die Risiken interner wie auch externer Betrugsversuche minimiert."
>
> ***Jörg Wiemer, Mitgründer und CSO der TIS***

Neben dem Sanction Screening hat TIS jüngst die Produktpalette um eine weitere innovative Lösung zur Betrugsprävention in RiskOptix erweitert – das Payee Community Screening (PCS). Das PCS arbeitet mit historischen Zahlungsdaten und Empfängerinformationen aus der TIS-Community global operierender Unternehmen und Banken, selbstverständlich anonymisiert und unter Einhaltung strengster Datenschutzauflagen. Durch eine enge Partnerschaft mit der Deutschen Bank wird die Anzahl der zugänglichen Daten signifikant erweitert: Auf etwa 100 Millionen zusätzliche Kontodaten kann das PCS hierdurch zugreifen.
Über die Kooperation mit der Deutschen Bank hat TIS damit auch Zugang zu SWIFTs erweitertem Pre-Validation-Service mit etwa 9 Milliarden anonymisierten Transaktionsnachrichten zwischen etwa 4 Milliarden globalen Konten pro Jahr.

PCS macht sich diese aggregierten Daten zunutze und screent alle durchlaufenden Zahlungen auf bekannte und validierte Kontoinformationen. Bei Abweichungen weisen Alerts in Echtzeit auf mögliche Verstöße hin. Rechnungsbetrug beispielsweise – eine Betrugsform, die in letzter Zeit stark zugenommen hat, bei der gefälschte Rechnungen eines Unternehmens mit abweichenden Empfängerangaben versendet werden – lässt sich hiermit effizient bekämpfen.

Das Besondere am PCS ist es, dass es sich kontinuierlich selbst verbessert. Das riesige Datenvolumen wächst über die zehntausenden täglich getätigten Zahlungen beteiligter Unternehmen in TIS beständig an. Die intelligente Sammlung, Verknüpfung und Auswertung dieser Daten beschleunigt die Erkennung von Betrugsversuchen, macht Zahlungen so noch sicherer und stellt ein sich selbst aktualisierendes und weiterentwickelndes Tool dar.

1. ZAHLUNGSAUFTRAG ERTEILEN

Unternehmen lösen Zahlungen an Lieferanten durch das System ihrer Wahl aus. Die Daten werden durch TIS weiter- geleitet oder in TIS erstellt.

2. GLOBALES SCREENING

TIS gleicht die Zahlungsangaben mit Daten in der umfangreichen Datenbank vergangener Unternehmenszahlungen der TIS-Community ab, also mit den anonymisierten Daten von PCS-Nutzern und Partnern von TIS.

3. VALIDIEREN ODER MARKIEREN

Durch den Abgleich der Empfänger und Accountdetails mit vergangen Zahlungen entscheidet TIS, ob eine Zahlung validiert werden kann oder ob sie aufgrund verdächtiger Informationen noch einmal geprüft werden muss.

4. AUSFÜHREN ODER PRÜFEN

Die autorisierten Nutzer in TIS können auf Basis der entsprechenden Hinweise entscheiden, ob eine Zahlung ausgeführt werden darf oder ob sie einer weiteren Prüfung unterzogen bzw. zurückgewiesen werden sollte.

ZUSAMMENFASSUNG

Das Thema *Cyber Security* hat sich laut der Horváth-Studie „CxO Priorities 2022" von Null auf Platz Zwei in der strategischen Agenda des C-Levels katapultiert. Insbesondere bei produzierenden Unternehmen steht nun die Sorge um einen sicheren, Compliance-konformen Zahlungsverkehr im Fokus. Anders als viele Finanzdienstleister und Versicherer, die in der Vergangenheit bereits häufig Opfer von Betrugsversuchen waren und folglich besser für diese Szenarien gerüstet sind, haben sie oft noch keine entsprechenden Lösungen implementiert. Den sich rapide entwickelnden Betrugsszenarien lässt sich am besten durch klare organisatorische Strukturen und Prozesse mit Unterstützung smarter, digitaler Lösungen begegnen. Diese sollten über die nötige Flexibilität und System-Konnektivität verfügen, um alle Entitäten und zahlungsrelevanten Systeme eines Unternehmens anbinden zu können, und bei organischem Wachstum wie auch bei M&As schnell mithalten. Auf der einen Seite ist es wichtig, dass lückenlose, Compliance-konforme Prozesse ermöglicht werden – und das auf einem globalen Level, quer über alle Geschäftseinheiten. Und auf der anderen Seite sollten sich diese Lösungen automatisiert updaten und beständig weiterentwickeln – so wie etwa das Sanction Screening und das PCS von TIS –, um neuen Betrugsszenarien der unterschiedlichsten Art schneller und effizienter begegnen zu können.

ÜBER HORVÁTH

Horváth ist eine international tätige, unabhängige Managementberatung mit mehr als 1.000 Mitarbeiterinnen und Mitarbeitern an Standorten in Deutschland, Österreich, der Schweiz, Ungarn, Rumänien, Italien, den USA, Saudi-Arabien und den Vereinigten Arabischen Emiraten. Wir stehen für ein ausgeprägtes Branchenverständnis sowie höchste fachliche Expertise in sämtlichen Unternehmensfunktionen – mit Fokus auf Performance Management und Transformation. Für unsere international agierenden Kunden führen wir weltweit Projekte durch. Dabei stellen wir auch durch die Zusammenarbeit mit unseren Partnerfirmen innerhalb der Beratungsallianz „Cordence Worldwide“ die genaue Kenntnis und Berücksichtigung der jeweiligen lokalen Gegebenheiten sicher. Cordence Worldwide ist ein globales Netzwerk von Beratungsunternehmen, die gemeinsam innovative Lösungen vorantreiben und umsetzen.

Unsere Consultants unterstützen Unternehmen und Führungskräfte mit umfassender Kompetenz in Geschäftsmodellen, Organisationsstrukturen, Prozessen und Systemen dabei, ihre Organisationen erfolgreich auf die Zukunft auszurichten. Mit Leidenschaft und Umsetzungsstärke verhelfen wir Veränderungen zum Erfolg, für das Gesamtunternehmen, für einzelne Unternehmensbereiche oder für Funktionen wie Vertrieb, Operations, Einkauf, Controlling & Finanzen, HR und IT. Horváth steht für Projektergebnisse, die nachhaltigen Nutzen und Wert schaffen. Deshalb begleiten unsere Beraterinnen und Berater Unternehmen von der betriebswirtschaftlichen Konzeption über die Verankerung in Prozessen und Systemen bis zum Change Management und Training von Führungs- und Fachkräften.

ÜBER TIS

TIS hat die Welt der Unternehmenszahlungen und des Cash Forecasting neu gedacht: mit einer Cloud-basierten Plattform, eigens dafür konzipiert, Ausgangszahlungen und alle damit verbundenen Prozesse zu optimieren.

Global agierende Organisationen, Konzerne und Finanzdienstleister setzen auf die Expertise von TIS für die Anbindung internationaler Banken und Konten, die Durchführung von Zahlungsprozessen sowie die die Analyse von Cashflow- und Compliance-Daten. Sie profitieren von einer ganzheitlichen Optimierung der zahlungsrelevanten Funktionen. Mit der TIS EPO Plattform steigern Unternehmen ihre operative Effizienz, während sie gleichzeitig Risiken minimieren, das Cash Forecasting verbessern, Working Capital-Transparenz erhalten und so einen strategischen Vorteil gewinnen.

Besuchen Sie tispayments.com und entdecken Sie, wie Ihr Unternehmen Enterprise Payment Optimization (EPO) erreichen kann.

TIS IN ZAHLEN

- **140+** LÄNDER
- **250+** B2B KUNDEN
- **300+** FACHKUNDIGE MITARBEITER
- **30,000+** NUTZER
- **1k+ Systeme** VERBUNDEN
- **100,000+** ZAHLUNGSPROFILE
- **11,000+** BANKEN- KONNEKTIVITÄTS-OPTIONEN
- **65,000+** BANKKONTEN
- **~25 Millionen** ZAHLUNGSEMPFÄNGER
- **$2 Billionen** JAHRESVOLUMEN
- **99.95%+** SYSTEM-VERFÜGBARKEIT
- **100%** NATIVE CLOUD

Alle Statistiken sind, sofern nicht anders angegeben, von Q3 2022

Enterprise Payments reimagined.

Learn more at tispayments.com »

TREASURY INTELLIGENCE SOLUTIONS GMBH

Germany (+49 6227 69824-0) | United States (+1 (617) 955 3223) | info@tispayments.com | tispayments.com