PART OF H1F
ADWEKO
IT's people's business.

Use Case:

Steigerung der Awareness in der Informationssicherheit durch IPA

Inhalt

1. Einleitung

1.1. Definition von Künstlicher Intelligenz (KI) und Robotic Process Automation (RPA)

Künstliche Intelligenz (KI) ist ein Teilgebiet der Informatik und bezieht sich auf die Fähigkeit von Maschinen oder Computern, diverse Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. Dabei werden verschiedene Ansätze verfolgt: Regelbasierte Systeme, die auf vordefinierten Abläufen beruhen, und maschinelles Lernen, bei dem Algorithmen durch große Datenmengen trainiert werden, um eigenständig Muster zu erkennen sowie Vorhersagen zu treffen. Dies ermöglicht es Maschinen, komplexere Aufgaben wie bspw. Spracherkennung, Bildverarbeitung sowie anspruchsvolle Entscheidungsprozesse zu bewältigen. *KI birgt somit in erheblichem Umfang das Potenzial, die tägliche Arbeit sowie die Arbeitswelt per se wesentlich zu transformieren, indem innovative Lösungen für diverse Herausforderungen erarbeitet werden.*

Robotic Process Automation (RPA), zu Deutsch „Robotergesteuerte Prozessautomatisierung", zielt darauf ab, Geschäftsprozesse durch Softwareroboter, auch "Bots" genannt, zu automatisieren bzw. abzubilden. Diese Bots können menschenähnliche Interaktionen mit digitalen Systemen imitieren, um bspw. Aufgaben wie Transaktionen, Kommunikation mit anderen Systemen oder wichtige Entscheidungsfindungsprozesse durchzuführen.

Die nachfolgende Abbildung zeigt übergreifend zusammengefasst, womit sich RPA u.a. beschäftigt und welche Chancen dadurch genutzt werden können.

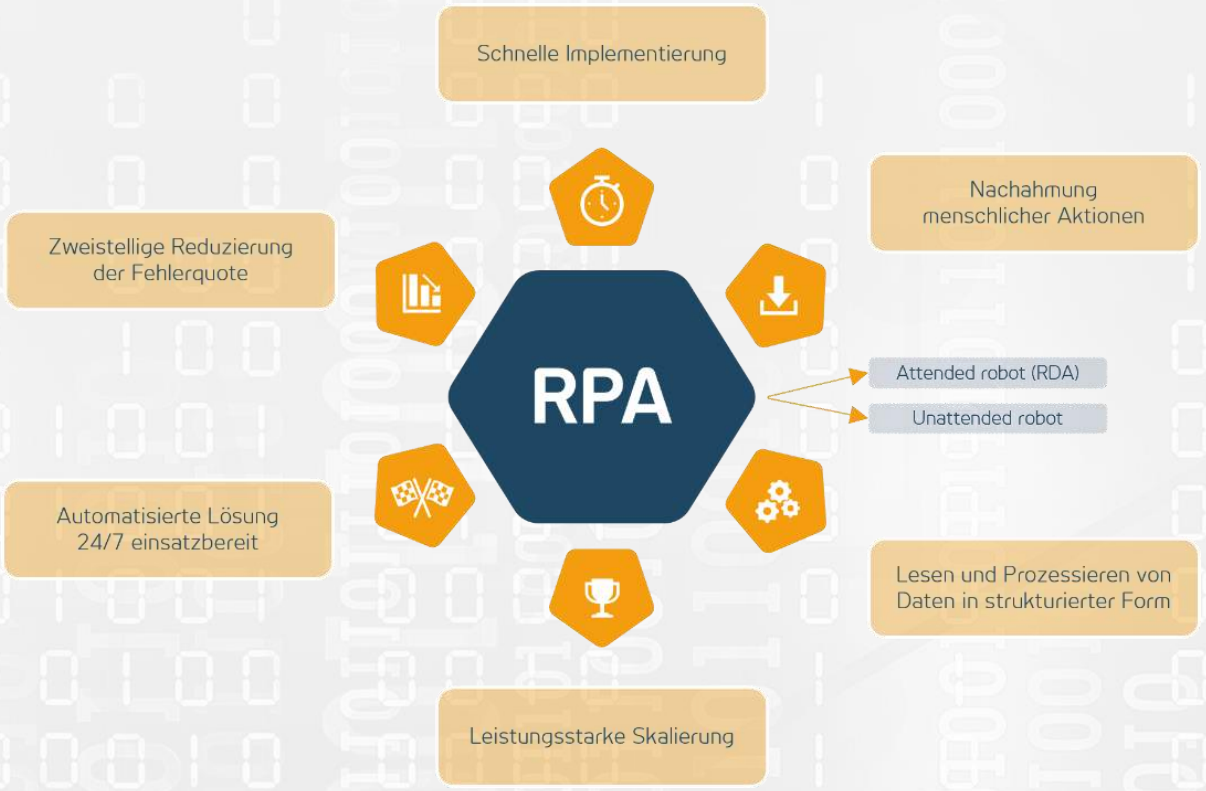


Abbildung 1: Was ist überhaupt Robotic Process Automation? (Quelle: Bereich Finance ADWEKO)

1.2. Bedeutung von Informationssicherheit im Kontext von KI und RPA

Die Bedeutung von Künstlicher Intelligenz (KI) und Robotic Process Automation (RPA) im Kontext Informationssicherheit ist von entscheidender Wichtigkeit, da diese Technologien sensible Daten verarbeiten und komplexe, automatisierte Prozesse steuern. Durch den Einsatz von KI werden große Datenmengen analysiert, während RPA repetitive Geschäftsprozesse automatisiert. In beiden Fällen besteht das Risiko des unbefugten Zugriffs, der Datenmanipulation oder Cyberangriffen ausgesetzt zu sein. Daher ist es unabdingbar, robuste und resiliente Sicherheitsmaßnahmen zu implementieren, um die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten und Prozesse zu gewährleisten. Unternehmen müssen sicherstellen, dass ihre Systeme vor Bedrohungen geschützt sind und gleichzeitig die Einhaltung gesetzlicher Vorschriften und Datenschutzstandards gewährleistet sind. *Nur durch eine umfassende Informationssicherheitsstrategie können die Chancen von KI und RPA voll ausgeschöpft werden, ohne die Sicherheit der Organisation zu gefährden.*

1.3. KI und RPA in Bezug auf Compliance, Datenschutz und ethische Aspekte

KI und RPA spielen eine signifikante Rolle bei der Optimierung von Compliance-Prozessen, indem sie sicherstellen, dass Unternehmen branchenspezifische Vorschriften erfüllen. Durch Automatisierung können Organisationen gewährleisten, dass ihre Aktivitäten den gesetzlichen Anforderungen entsprechen, sei es im Finanzsektor, im Versicherungswesen oder in anderen regulierten Bereichen. Dank dieser Technologien können Unternehmen Prozesse präzise protokollieren und nachverfolgen, was wiederum die Bereitstellung von überzeugenden Nachweisen für die Einhaltung ihrer Compliance-Richtlinien erleichtert.

Aufgrund der Verarbeitung großer Mengen sensibler Daten durch KI und RPA ist Datenschutz von höchster Priorität. Unternehmen müssen gewährleisten, dass Daten sicher gespeichert, übertragen und verarbeitet werden. Datenschutzregelungen wie die DSGVO in der Europäischen Union setzen strikte Vorschriften für den Umgang mit personenbezogenen Daten. Es liegt in der Verantwortung der Unternehmen, sicherzustellen, dass ihre KI- und RPA-Systeme diesen Standards entsprechen, um Datenschutzverletzungen zu verhindern.

Ethische Überlegungen spielen ebenso eine entscheidende Rolle, insbesondere im Kontext von Künstlicher Intelligenz (KI). Algorithmen können aufgrund der Daten, mit denen sie trainiert werden, Vorurteile entwickeln, die zu diskriminierenden oder ethisch fragwürdigen Entscheidungen führen können. Unternehmen müssen sicherstellen, dass ihre KI-Systeme transparent, fair und verantwortungsbewusst sind. Dies erfordert eine gründliche Überprüfung der Datenquellen und eine kontinuierliche Überwachung der Algorithmen, um sicherzustellen, dass sie ethischen Standards genügen.

Im Großen und Ganzen ist es entscheidend, dass Unternehmen bei der Implementierung von KI und RPA nicht nur technologische und fachliche Aspekte berücksichtigen, sondern auch Compliance, Datenschutz und ethische Fragen im Blick behalten. Dies erfordert eine enge Zusammenarbeit zwischen IT-Experten, Datenschutzbeauftragten und Ethikkomitees, um sicherzustellen, dass diese Technologien im Einklang mit den rechtlichen und ethischen Standards betrieben werden. Nur so können die Vorteile von KI und RPA voll ausgeschöpft werden, ohne die Integrität und den Ruf des Unternehmens zu gefährden.

2. Potenziale der Nutzung von KI in Verbindung mit RPA in der Informationssicherheit

Die Nutzung von KI in Verbindung mit RPA bietet im Bereich der Informationssicherheit zahlreiche Einsatzmöglichkeiten und Potenziale. Nachfolgend soll dies durch Beispiele aufgezeigt werden.

- Frühzeitige Bedrohungserkennung: KI kann genutzt werden, um große Datenmengen aus verschiedenen Quellen in Echtzeit zu analysieren und potenzielle Sicherheitsbedrohungen zu identifizieren. Dies ermöglicht eine frühzeitige Erkennung von Angriffen und schädlichen Aktivitäten.
- Automatisierte Reaktion auf Bedrohungen: RPA kann in Kombination mit KI verwendet werden, um auf erkannte Sicherheitsbedrohungen automatisch zu reagieren. Dies kann beispielsweise bedeuten, dass RPA-Bots bestimmte Schutzmaßnahmen aktivieren, Benutzerkonten sperren oder Sicherheitslücken schließen – all dies ohne menschlichen Eingriff.
- Sicherheitsüberwachung rund um die Uhr: RPA kann Aufgaben im Zusammenhang mit der Sicherheitsüberwachung automatisieren, was eine kontinuierliche Überwachung und Analyse von Sicherheitsereignissen ermöglicht, auch außerhalb der regulären Arbeitszeiten.
- Schulung und Sensibilisierung: KI kann genutzt werden, um personalisierte Schulungs- und Sensibilisierungsprogramme zu entwickeln, um Mitarbeiter:innen in Bezug auf ihr Sicherheitsbewusstsein zu schulen und zu testen.

Die Kombination von KI und RPA in der Informationssicherheit bietet also die Möglichkeit, Sicherheitsprozesse zu optimieren, Bedrohungen effektiver zu erkennen und schneller darauf zu reagieren, was letztendlich zur Stärkung der Gesamtsicherheit beiträgt. Im nachfolgenden Abschnitt wird der Punkt „Schulung und Sensibilisierung" durch einen Use-Case praktisch verdeutlicht.

3. Use-Case Einsatz von KI und RPA - Phishing Simulation

Bei ADWEKO wurde durch die Zusammenarbeit der Bereiche IT-Security Management und Finance (Fokusgruppe „Prozessoptimierung") ein Use-Case entwickelt, um das Zusammenspiel von KI und RPA im Kontext der Informationssicherheit praktisch um- und einzusetzen. Ziel ist es, das Verhalten der Mitarbeiter:innen in Reaktion auf eine Phishing-E-Mail zu analysieren und die Reaktionen sowie ihre Auswirkungen zu untersuchen.

Fachliche Vorgaben

- Ethische Durchführung: Es ist entscheidend, dass die Phishing-Simulation ethisch und verantwortungsvoll erfolgt. Die gefälschten Phishing-E-Mails sollten keine Angst oder Panik bei den Mitarbeiter:innen auslösen. Mitarbeiter:innen sollten über die Kampagne informiert werden, sobald sie auf die Simulation reagieren.
- Realistisches Phishing-Szenario: Die Phishing-Simulation sollte ein realistisches Szenario nachahmen, das in der Organisation auftreten könnte. Dies hilft den Mitarbeiter:innen, sich besser auf echte Bedrohungen vorzubereiten.
- Feedback und Schulungsmöglichkeiten: Nach der Phishing-Simulation sollten den Mitarbeiter:innen Feedback und Schulungsmöglichkeiten angeboten werden. Dies kann dazu beitragen, dass die Mitarbeiter:innen aus ihren Fehlern lernen und ihre Fähigkeiten zur Erkennung von Phishing-Angriffen verbessern.
- Daten und Metriken sammeln: Während der Kampagne sollten Daten und Metriken gesammelt werden, um die Wirksamkeit der Schulung zu messen. Dies kann die Anzahl der gemeldeten Phishing-E-Mails, die Klickrate auf Phishing-Links und die Verbesserung der Erkennungsrate umfassen. Dabei werden lediglich teilanonymisierte Daten berücksichtigt.
- Regelmäßige Wiederholung: Die Phishing-Simulation sollte regelmäßig wiederholt werden, um sicherzustellen, dass das Sicherheitsbewusstsein der Mitarbeiter:innen aufrechterhalten und gestärkt wird.

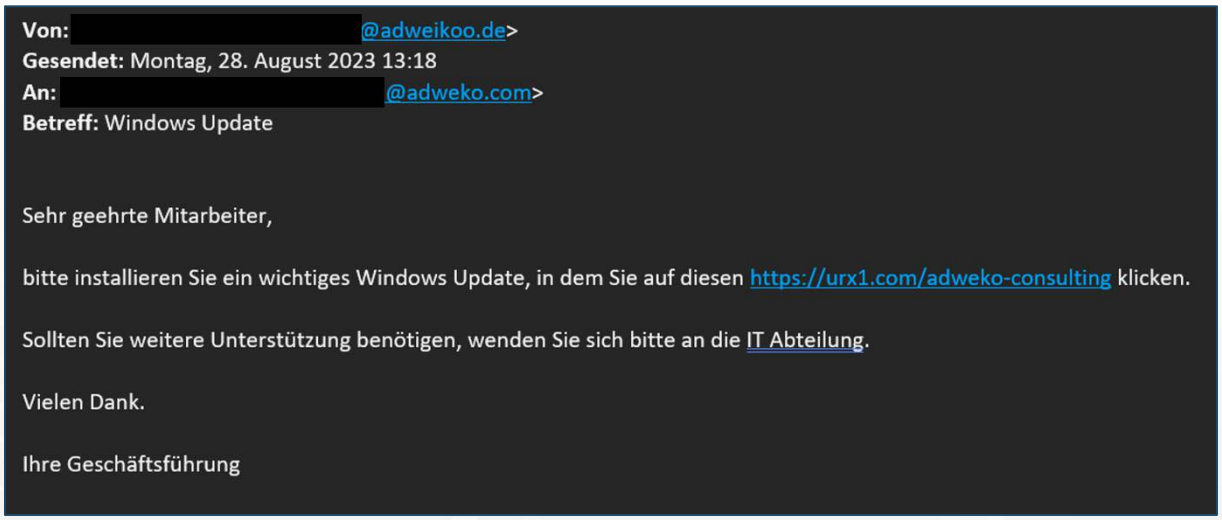
Technische Umsetzung

Der E-Mail-Text wird durch Künstliche Intelligenz anhand der Anbindung der offiziellen OpenAI-API formuliert und enthält einen speziellen Link. Dieser Link ermöglicht es, nachzuvollziehen, wie oft und wann dieser angeklickt wurde. Zum Versenden der Mails an die Mitarbeiter:innen nutzt der Roboter einen SMTP-Server. Der Bot schreibt die dokumentationsrelevanten Angaben, bspw. den Zeitpunkt des Versendens einer E-Mail oder wie oft der Link seit dem letzten Durchlauf geöffnet wurde, in eine Excel-Datei. Die Simulation wird teilanonymisiert durchgeführt, d.h. es werden keine Namen von Mitarbeiter:innen verwendet. Obwohl die Themen der E-Mails festgelegt sind, kann der Bot den Textinhalt bei jeder Mail unterschiedlich generieren, um dadurch die Situation realistischer zu formulieren und so weniger Verdacht, sowohl bei internen ADWEKO-Mitarbeiter:innen als auch beim E-Mail-Filter zu erwecken.

Operational Effectiveness

Die Phishing Simulation in diesem Format wird im Rahmen der internen Awarness Kampagne bei ADWEKO erstmalig im Jahr 2024 zum Einsatz kommen. Sie wird ein wesentlicher Bestandteil, im Kontext der Sensibilisierung der Mitarbeiter:innen auf informationssicherheitsrelevante Themen, sein. Darüber hinaus stellen wir sicher, dass damit auch Anforderungen aus der Regulatorik - wie etwa der ISO 27001 - erfüllt werden.

Beispiele von KI generierten Texten



Von: [redacted]@adweikoo.de>
Gesendet: Montag, 28. August 2023 13:18
An: [redacted]@adweko.com>
Betreff: Windows Update

Sehr geehrte Mitarbeiter,

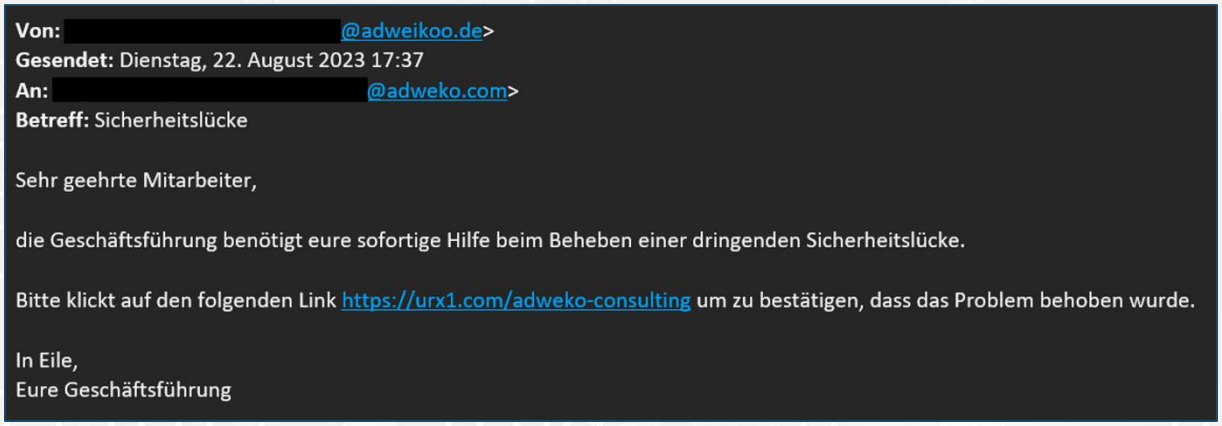
bitte installieren Sie ein wichtiges Windows Update, in dem Sie auf diesen https://urx1.com/adweko-consulting klicken.

Sollten Sie weitere Unterstützung benötigen, wenden Sie sich bitte an die IT Abteilung.

Vielen Dank.

Ihre Geschäftsführung

Abbildung 2 KI-generierte E-Mail zur Erinnerung eines Software-Updates



Von: [redacted]@adweikoo.de>
Gesendet: Dienstag, 22. August 2023 17:37
An: [redacted]@adweko.com>
Betreff: Sicherheitslücke

Sehr geehrte Mitarbeiter,

die Geschäftsführung benötigt eure sofortige Hilfe beim Beheben einer dringenden Sicherheitslücke.

Bitte klickt auf den folgenden Link https://urx1.com/adweko-consulting um zu bestätigen, dass das Problem behoben wurde.

In Eile,
Eure Geschäftsführung

Abbildung 3 KI-generierte E-Mail mit Hinweis auf eine Sicherheitslücke im Unternehmen

4. Challenges bei der Nutzung von KI und RPA in der Informationssicherheit

Komplexität der Systeme und benötigte Ressourcen

Eine erfolgreiche Implementierung sowie der Betrieb von KI-Algorithmen und RPA-Plattformen erfordern ein profundes technisches Know-how und spezialisiertes Prozesse-Knowledge, um sie effizient in komplexen Systemen einzusetzen. Als Konsequenz daraus erhöht sich der Bedarf an Ressourcen im Unternehmen, um diesen Entwicklungen zu begegnen.

Datenschutz und ethische Aspekte bei der Verarbeitung von Daten

KI- und RPA-Systeme verarbeiten vertrauliche Daten, was Datenschutzherausforderungen mit sich bringen und die dringende Notwendigkeit zur strikten Einhaltung gesetzlicher Bestimmungen wie der DSGVO, die einen wichtigen Platz einnehmen muss.

Mangelnde Transparenz und Erklärbarkeit von KI-Algorithmen

KI-Modelle sind häufig kompliziert und schwer verständlich. Es gestaltet sich herausfordernd nachzuvollziehen, wie sie zu spezifischen Entscheidungen gelangen, was zu Problemen bei der Fehlersuche und zur Beeinträchtigung des Vertrauens der Nutzer führen kann.

Bedrohungen durch KI und RPA?

Auch Kriminelle können KI und RPA nutzen, um gezielte Angriffe auf Unternehmen durchzuführen. Sie könnten bspw. Angriffe automatisieren oder KI-Algorithmen entwerfen, um Schwachstellen in Sicherheitssystemen zu identifizieren. Unternehmen müssen sich gegen solche Bedrohungen schützen.

Fehler und Fehlalarme

KI-Systeme sind nicht perfekt und können falsche Entscheidungen treffen oder Fehlalarme auslösen. Dies kann dazu führen, dass Sicherheitsanalysten Zeit und Ressourcen für die Untersuchung von Fehlalarmen aufwenden, anstatt sich auf echte Bedrohungen zu konzentrieren.

Widerstand gegen Veränderung

Die Integration von KI und RPA in bestehende Sicherheitsprozesse kann auf Widerstand stoßen, insbesondere wenn nicht ausreichend über die Chancen sowie Möglichkeiten aufgeklärt wird oder wenn ein effektives Change-Management fehlt. Mitarbeiter:innen könnten somit besorgt sein, dass ihre Arbeitsplätze durch Automatisierung gefährdet sind.

5. Zusammenfassung und Ausblick

5.1. Zusammenfassung der wichtigsten Punkte

Durch den Einsatz von KI in der Informationssicherheit ist es möglich, Bedrohungen frühzeitig zu erkennen. Die KI kann große Datenmengen analysieren, um potenzielle Sicherheitsbedrohungen zu identifizieren und Alarme auszulösen. Darüber hinaus ist es durch RPA möglich, auf erkannte Bedrohungen automatisiert zu reagieren, um geeignete Sicherheitsmaßnahmen zu aktivieren und schädliche Aktivitäten zu blockieren. Auch für den Einsatz einer Awareness Kampagne kann die Kombination beider Technologien genutzt werden, um die Sensibilisierung der Mitarbeiter:innen gegenüber Phishing Attacken zu schärfen. Der Einsatz von KI in Verbindung mit RPA stärkt die Informationssicherheit, indem sie die Reaktionsgeschwindigkeit auf Bedrohungen erhöht, Mitarbeiter:innen schult, Schwachstellen reduziert und insgesamt die Sicherheitslage in einer Organisation verbessert.

5.2. Ausblick auf zukünftige Entwicklungen im Bereich KI & RPA in der Informationssicherheit

Der Bereich der Künstlichen Intelligenz (KI) und Robotic Process Automation (RPA) wird in Bezug auf Informationssicherheit weiterhin bedeutende Fortschritte machen. In der Zukunft sind wichtige Trends und Entwicklungen zu erwarten, die diesen Fortschritt vorantreiben. Einige mögliche Schlüsseltrends und Entwicklungen, die erwartet werden, sind:

Erweiterte Authentifizierungsmethoden

KI und RPA werden genutzt, um fortschrittliche Authentifizierungsmethoden zu entwickeln, die sicherer und benutzerfreundlicher sind. Dabei könnten biometrische Daten, Verhaltensanalysen und kontinuierliche Echtzeit-Authentifizierung breiter eingesetzt werden, um den Zugriff auf sensible Daten zu sichern.

Automatisierte Reaktion auf Sicherheitsvorfälle

RPA wird verwendet, um automatisch auf Sicherheitsvorfälle zu reagieren. Bei der Erkennung eines Angriffs können RPA-Systeme unverzüglich vordefinierte Maßnahmen ergreifen, um den Angriff einzudämmen und den Schaden zu minimieren. Dies ermöglicht eine schnellere Reaktion auf Bedrohungen.

Quantencomputing und Kryptographie

Durch den Fortschritt im Bereich des Quantencomputings werden neue Verschlüsselungsmethoden erforderlich sein, um sicherzustellen, dass Daten vor zukünftigen Angriffen, die auf Quantencomputern basieren, geschützt sind. Künstliche Intelligenz wird eine entscheidende Rolle dabei spielen, indem sie dazu beiträgt, zuverlässige Verschlüsselungssysteme zu entwickeln und bestehende Sicherheitsprotokolle zu stärken.

Insgesamt wird die Rolle von KI und RPA in der Informationssicherheit und Prozessautomatisierung entscheidend sein, da sie fortschrittliche Technologien bereitstellen und somit eine transformative Wirkung entfalten. Durch den Einsatz dieser Technologien können Unternehmen aufzunehmend komplexe Bedrohungen reagieren und gleichzeitig sicherstellen, dass Datenschutz und ethische Standards auch in Zukunft gewahrt bleiben. Dies verdeutlicht den stetigen Fortschritt und die zukunftsweisenden Möglichkeiten, die sich im Bereich der Informationssicherheit durch KI und RPA eröffnen.

6. Ihre Ansprechpartner:innen

Unser Services für Sie

Durch unsere Expertise in der Informationssicherheit bieten wir mit unseren Leistungen nicht nur Schutz vor potenziellen Gefahren, sondern schaffen auch eine Grundlage für nachhaltigen Geschäftserfolg durch das Vertrauen Ihrer Kunden in die Integrität Ihrer Daten und Systeme. Falls Sie weitere Einzelheiten oder spezifische Informationen benötigen, sind wir gerne für Sie da. Kontaktieren Sie uns bitte, damit wir Ihnen persönlich weiterhelfen können.

Kontaktieren Sie bei Fragen gerne:

Christopher Schedel

Autor und Experte im Bereich IT-Security

Fahri Can

Autor und Experte im Bereich IT-Security

Dominica Bengs

Topic Lead Finance Fokusgruppe "Prozessoptimierung"

Dogukan Dogan

Automatisierungsexperte