eleks

TOP 10 RPA-SICHER-HEITSRISIKEN

Einleitung

Die Robotic Process Automation (RPA) ist eine aufstrebende Technologie, mit der sich vom Menschen durchgeführte Routineoperationen automatisch über ein Graphical User Interface (GUI) erledigen lassen.

In ihrer Grundform stellt die RPA den nächsten Entwicklungsschritt von in Anwendungen eingebetteten Skripten dar. Die Ausführung erfolgt jedoch auf einer eigenen Plattform und ermöglicht so anwendungsübergreifende Aktivitäten. Mit APIs (Application Programming Interfaces) lassen sich die gleichen Ergebnisse erzielen, allerdings stellt die häufig in Unternehmen verwendete Software solche Funktionen meistens nicht bereit.

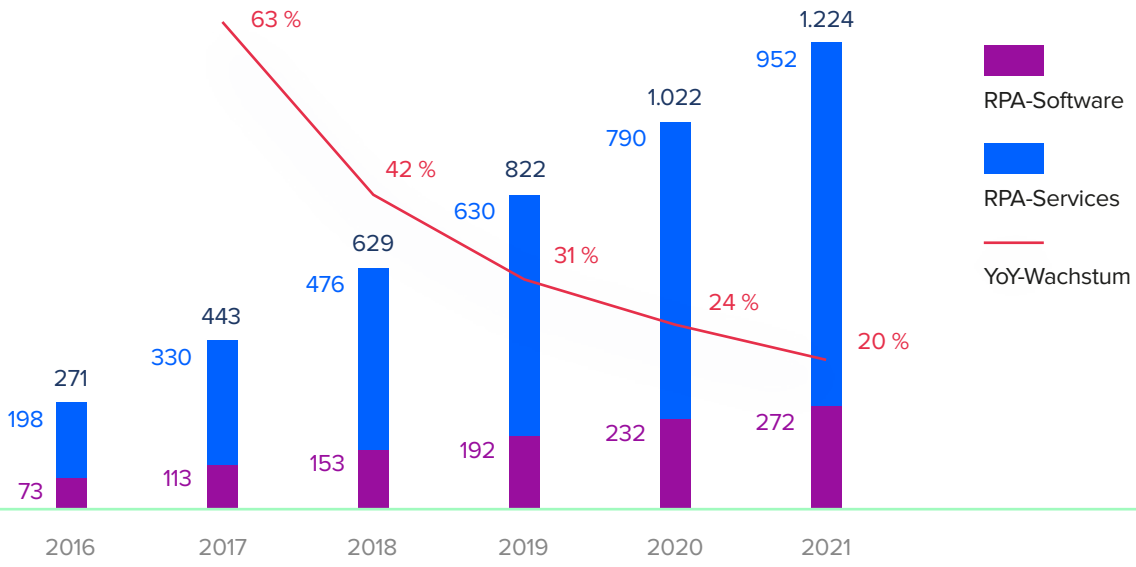
Software-Roboter ermöglichen eine **schnellere Überwindung aktueller Beschränkungen und sind dazu noch viel günstiger** als die Neuentwicklung von Systemen. Ein weiterer Vorteil der RPA-Implementierung liegt in der **Reduzierung von Betriebskosten** durch den Wegfall von Personalausgaben.

Umsatzprognose für den RPA-Markt bis 2021:

1,2 Milliarden $

Der globale RPA-Markt, 2016–2021 (in Millionen US-Dollar)

Laut HfS Research Ltd.



Software-Roboter werden in zwei Kategorien unterteilt: unterstützte und nicht unterstützte.

Unterstützte RPA trägt zum Prozess bei, manche Aktionen müssen aber von einem Mitarbeiter ausgeführt werden. Ohne menschliches Zutun funktioniert es nicht.

Nicht unterstützte RPA ermöglicht einen unbemannten Betrieb bzw. eine vollautomatische Ausführung der Aufgabe.

Der nächste Schritt in der Entwicklung der RPA-Technologie ist die **kognitive** RPA, die durch Algorithmen des maschinellen Lernens sowohl zur Entscheidungsfindung als auch zur Selbstoptimierung beiträgt.

Software-Roboter stehen kurz vor dem Marktstart. Deshalb sollten Firmen geeignete RPA-Implementierungs-Rahmenbedingungen schaffen, um mit den Risiken schon im Vorfeld effizient umzugehen.

Sonst kann es zu Sicherheitsvorfällen, Geschäftsausfällen und dem Problem kommen, dass man aufgrund der Komplexität der RPA-Umgebung später keine geeigneten Kontrollen mehr integrieren kann.

RPA ähnelt dem End User Computing, wobei sich die Wiederverwendung eines angepassten Kontroll-Frameworks als der vernünftigste Ansatz erweist. Alternativ können Sie auch Steuerelemente verwenden, die für intern entwickelte Anwendungen konzipiert wurden. Der größte Unterschied zwischen Software-Robotern und Anwendungen ist die IAM-Domain (Identity Access Management). RPA-Instanzen ähneln in ihrem Verhalten einem individuellen Benutzer. Indem Firmen sowohl für Software-Komponenten als auch IAM effiziente Kontrollen entwickeln und implementieren, können sie leicht eine gut kontrollierbare Umgebung für RPA-Technologie erstellen.

Auf der anderen Seite gilt für kognitive RPA eine andere Bedrohungslage, die in der aktuellen Version der internationalen IT-Sicherheitsstandards nur unzureichend abgedeckt ist. Dazu zählen zum Beispiel Probleme mit der Zuverlässigkeit von Machine-Learning-Algorithmen.

Diese Herausforderungen erfordern die Schaffung eines neuen Kontrollrahmens, der auf internen Best Practices, der Zusammenarbeit mit anderen Unternehmen und Beratern sowie proaktiven Diskussionen mit den Aufsichtsbehörden basiert.

Bedrohungen der RPA-Sicherheit

Im weiteren Verlauf dieses Whitepapers erfahren Sie, welche Gefahren auf die RPA-Technologie lauern. Diese Bedrohungen wurden in Bereiche unterteilt und beziehen sich auf den BSI-Katalog. Zwecks besserer Verständlichkeit wurden sie zusammen mit den entsprechenden Szenarien illustriert.

eleks

01

Unzureichende RPA-Kontrolle

T 0.18 Falsche Planung oder mangelnde Anpassung

SZENARIO:

Ihre Firma verwendet RPA schon länger und entscheidet sich, IT-Risiken von einem unabhängigen Anbieter bewerten zu lassen. Im Bericht dieser renommierten Beratungsfirma steht, dass die geschätzten Kosten für die Behebung aktueller RPA-Probleme dem Nettoeinkommen Ihres Unternehmens aus dem vergangenen Jahr entsprechen. Der Grund: Zahlreiche kaum durchdachte, selbst entwickelte, minderwertige RPA-Programme, die in vielen Abteilungen zum Einsatz kommen.

BEDROHUNGSDETAILS:

Unternehmen haben heutzutage mit Schatten-IT zu kämpfen und sind aufgrund mangelnder Ressourcen nicht in der Lage, ihre Vermögenswerte ordnungsgemäß zu ermitteln. Hinzu kommen noch viele alte Software-Anwendungen, die nur schwer zu verwalten, zu pflegen und zu schützen sind. RPA ist so konzipiert, dass sie auch für IT-fremde Mitarbeiter eine einfache Erstellung ermöglicht. Wenn die Technologie nicht über Kontrollmechanismen verfügt, kann es passieren, dass Sie es in kurzer Zeit mit einer Unmenge an Software-Robotern zu tun bekommen, die erhebliche Risiken darstellen.

Deshalb kann es passieren, dass kurzfristige Vorteile aus der anfänglichen RPA-Verankerung über einen längeren Zeitraum zu Verlusten und einer Zunahme der Schatten-IT im Unternehmen führen.

Wenn die RPA-Technologie nicht kontrolliert wird, kann es sein, dass Sie es in kurzer Zeit mit einer Unmenge an Software-Robotern zu tun bekommen, die erhebliche Risiken darstellen.

02

Ineffiziente RPA-Implementierung

T 0.18 Falsche Planung oder mangelnde Anpassung, T 0.27 Mangel an Ressourcen

SZENARIO:

Ihr Wettbewerber erwähnt in einer Pressemitteilung, dass er schon im dritten Quartal des Geschäftsjahres deutlich die Kosten senken konnte. Sie wissen, dass der Hauptfaktor für diesen Erfolg eine stabile RPA-Implementierung ist. Allerdings zeichnen sich in Ihrer Firma kaum Fortschritte bei der Entwicklung von Software-Robotern ab – trotz eines kürzlich vorgestellten Prämienprogramms. Eine Reihe von Robotern, die in Produktion gegangen sind, scheinen nicht effizient zu arbeiten – die tatsächlichen Einsparungen bleiben klar hinter den Erwartungen zurück.

BEDROHUNGSDETAILS:

Zu den Vorteilen der RPA zählt die Möglichkeit, die Kosten zu senken, indem die Anzahl der zur Unterstützung des neu automatisierten Prozesses erforderlichen Vollzeitstellen reduziert wird. Für das Unternehmen ist dies natürlich ein erstrebenswertes Ziel. Allerdings kann man nicht von jedem Mitarbeiter erwarten, dass er dafür Enthusiasmus an den Tag legt, wenn dadurch sein Arbeitsplatz wegfällt.

Falls die Rollen bei der RPA-Implementierung nicht korrekt zugewiesen werden, kann es zu Interessenkonflikten kommen. Zusätzliche Probleme können auftreten, wenn keine Priorisierung für RPA-Projekte existiert oder am Projekt beteiligte Kollegen keine Technologiekenntnisse besitzen und ihre Vorteile nicht umsetzen können.

Falls die Rollen bei der RPA-Implementierung nicht korrekt zugewiesen werden, kann es zu Interessenkonflikten kommen.

03

Lücken bei IAM-Kontrollen

T 0.23 Unerlaubter Zugriff auf IT-Systeme, T 0.32 Berechtigungsmissbrauch

SZENARIO:

Daten Ihres CRM-Systems (Client Relationship Management) wurden gestohlen und auf dem Schwarzmarkt verkauft. Nach eingehender Untersuchung stellt sich heraus, dass die Datenverletzung auf internen Betrug zurückzuführen ist: Die Daten wurden von einem ehemaligen Mitarbeiter mithilfe einer in einer Backoffice-Abteilung entwickelten RPA extrahiert.

BEDROHUNGSDETAILS:

Es existieren einige einfache Methoden zur Handhabung von RPA-Berechtigungen. So kann man festlegen, dass Roboter nur im Zusammenhang mit Benutzerkonten oder einem gemeinsamen technischen Anwender eingesetzt werden können. Diese Praktiken zählen vom Sicherheitsaspekt her allerdings zu den eher riskanten Optionen.

Gibt es keine einheitlichen, sicheren und effizienten IAM-Praktiken für Software-Roboter, ermöglicht das internen Betrug. Auch die Anfälligkeit für Hacker-Attacken steigt. Darüber hinaus führt es zur Missachtung der behördlich vorgeschriebenen Aufgabentrennung.

Gibt es keine einheitlichen, sicheren und effizienten IAM-Praktiken für Software-Roboter, ermöglicht das internen Betrug.

04 Mangelnde Vorbereitung auf Pannen

T 0.40 Dienstverweigerung, T 0.11 Fehlfunktionen/Unterbrechungen bei Serviceanbietern

SZENARIO:

Schon den dritten Tag nacheinander kann Ihre Firma Kundenaufträge nicht bearbeiten. Die RPA-Technologie, mit der Kundenanfragen über eine Online-Plattform verarbeitet werden, funktioniert aus unbekannten Gründen nicht mehr. Die Mitarbeiter können die Arbeitslast nicht bewältigen.

BEDROHUNGSDETAILS:

Nach ihrer Einsetzung können Software-Roboter den Workflow und die Ressourcen negativ beeinflussen. Wenn die RPA nicht an ein Business-Continuity-Programm geknüpft ist, kann der Ausfall eines einzigen Roboters Ihre Firma in eine Krise stürzen.

Eine weitere Bedrohung für die Stabilität der Infrastruktur des Unternehmens ist die Abhängigkeit von der Software, mit der RPA erstellt wird. Fehler in einem RPA-Software-Update oder die Insolvenz des Software-Anbieters können sogar noch schlimmere Konsequenzen haben, falls dann die Mehrheit der Software-Roboter nicht mehr funktioniert. Wie bereits erwähnt, besteht eine der besten RPA-Einsatzmöglichkeiten darin, die Schwachpunkte älterer Systeme zu beheben. Dadurch kann Ihre Firma zwar die Migration auf ein neueres System herauszögern, dies sollte aber nicht die Sanierung von EOL/EOS-Anwendungen beeinträchtigen. Ansonsten kann dies zu Ausfällen veralteter Komponenten führen.

Wenn die RPA nicht an ein Business-Continuity-Programm geknüpft ist, kann der Ausfall eines einzigen Roboters Ihre Firma in eine Krise stürzen.

05

Schlechtes Change Management

T 0.25 Ausfall von Geräten oder Systemen

SZENARIO:

Am heutigen Tag hat Ihre Firma 100-mal mehr Produkte verkauft als an jedem anderen Tag des vergangenen Jahres. Ein Grund zum Feiern? Kaum, denn die Bestellungen wurden zu einem viel zu niedrigen Preis angenommen und verarbeitet, als auf der Website ausgewiesen. Dazu wurden manche von ihnen bereits ausgeliefert. Immerhin hat die IT-Abteilung den Fehler bereits gefunden: Die RPA hat nach einem Update des CRM-Systems Fehler bei der Datenextraktion gemacht, was die Position mancher Datenzeilen in der Benutzeroberfläche (GUI) beeinträchtigte.

BEDROHUNGSDETAILS:

Software-Roboter gelten als zusätzliche Asset-Klasse und sollten in den Change-Management-Prozess eingebunden werden. Ansonsten kann es zu Serviceausfällen und/oder Bearbeitungsfehlern kommen, was auch an zu wenig dokumentierten Abhängigkeiten von RPA in Bezug auf andere Software-Komponenten liegen kann. Bei kognitiver RPA ist die Situation noch komplizierter, weil sie – im Gegensatz zu anderen Algorithmen des maschinellen Lernens – einen spezifischen Change-Management-Ansatz erfordert. Selbst verschuldete Code- und Algorithmus-Änderungen durch die Verarbeitung neuer Datensätze stellen eine weitere mögliche Fehlerquelle dar.

Wenn Sie keinen Change-Management-Prozess für RPA implementieren, kann es zu Service-ausfällen und/oder Bearbeitungsfehlern kommen.

06

Ungenügendes Schwachstellen-Management

T 0.28 Software-Schwachstellen oder -Fehler, T 0.23 Unerlaubter Zugriff auf IT-Systeme

SZENARIO:

Das rote Team meldet ein schwerwiegendes Problem, das im Rahmen des aktuellen Eindringtests im Netzwerkumfeld festgestellt wurde. Es liegt anscheinend eine Schwachstelle beim Push-Update-Mechanismus der RPA-Freeware vor. Diese Schwachstelle existiert schon länger, wurde vom Software-Anbieter aber nie behoben. Die Anwendung kommt in einigen Abteilungen in erster Linie bei der Entwicklung von Robotern zum Einsatz. Die weitere Untersuchung bringt ein zusätzliches Problem mit in Klartext gespeicherten RPA-Passwörtern ans Tageslicht.

BEDROHUNGSDETAILS:

Sowohl RPA-Software als auch -Instanzen stellen zusätzliche Angriffsflächen dar. Angesichts der schnellen Verbreitung der Roboter-Technologie lässt sich vorhersagen, dass Unternehmen durch sie in Zukunft großen Gefahren ausgesetzt sind. Dies wird die Nachfrage nach Schwachstellen bei RPA-Software auf dem Schwarzmarkt nach oben treiben und die Technologie zu einem Ziel für Hacker machen.

Sowohl RPA-Software als auch -Instanzen stellen zusätzliche Angriffsflächen dar.

Auch über das Passwort-Management für Software-Roboter müssen wir sprechen: Wenn dieses nämlich nicht korrekt gemäß den Richtlinien Ihrer Firma gehandhabt wird, öffnet das Tor und Tür für internen Betrug. Darüber hinaus können Hacker viele Prozesse im großen Rahmen angreifen, nachdem sie sich Zugang zum System verschafft haben.

07

Uneinheitliche RPA-Ergebnisse

T 0.18 Falsche Planung oder mangelnde Anpassung, T 0.27 Mangel an Ressourcen

SZENARIO:

Angesichts der Ergebnisse des Prüfungsberichts für Ihr Unternehmen fällt es Ihnen schwer, die für die inkorrekte Steuerdeklarierung der letzten beiden Jahre auferlegten Geldbußen zu akzeptieren. Die Rundungsregeln wurden bei einem Software-Update falsch konfiguriert. Mitarbeiter der Buchhaltung hätten den Fehler sofort erkannt, allerdings wird die Berichterstattung aktuell mit nicht unterstützter RPA durchgeführt, die nicht über die gleiche Flexibilität verfügen.

BEDROHUNGSDETAILS:

Die automatische Ausführung von Prozessen durch RPA kann zu zahlreichen Problemen und somit Datenfehlern führen. Hier folgen einige Beispiele:

- Fehlkonfigurationen und Bugs bei der RPA
- unvorhersehbare Änderungen im Modell der kognitiven RPA
- mangelnde Flexibilität des RPA-Algorithmus beim Umgang mit Ausnahmen

Deshalb wird es ohne Vorproduktionstests und/oder regelmäßige Prüfungen irgendwann zu einem Verlust der Datenintegrität kommen. Das kann aber auch passieren, wenn zur Ausführung durch den Menschen bestimmte Aufgaben von der RPA-Technologie übernommen werden.

Ohne Vorproduktionstests und/oder regelmäßige Prüfungen wird es irgendwann zu einem Verlust der Datenintegrität kommen.

08

Nichteinhaltung von Gesetzen

T 0.29 Verletzung von Gesetzen oder Vorschriften, T 0.38 Missbrauch persönlicher Daten

SZENARIO:

Ein Verweis auf die Black Box ist weit von dem entfernt, was Regulierungsbehörden als Erklärung für das von Ihrem Unternehmen verwendete Risikomodell erwarten. Auch wenn Sie stets das höchste Maß an Sicherheit bei der kognitiven RPA im Auge haben, die Sie für die Bewertung der Kreditnehmer verwenden, fällt es schwer, sie in das bisherige Regelwerk einzupassen. Onsite-Buchprüfer sind mit dem Konzept des maschinellen Lernens nicht vertraut und vermerken dann folglich in ihrem Bericht, dass das Kreditrisiko überhaupt nicht gemanagt wird.

BEDROHUNGSDETAILS:

Ungewissheiten des regulatorischen Rahmenwerks (in Bezug auf Innovationen) sind ein Hindernis für die Installierung moderner Technologien. Wenn Sie nicht in der Lage sind, Aufsichtsbehörden mit Software-Robotern erstellte Ergebnisse zu erklären, kann das Geldbußen oder sogar den Verlust der Lizenz für den Markt bedeuten. Ein ähnliches Problem besteht bei der Bereitstellung von Nachweisen eines formellen Zusammenhangs zwischen von der RPA ausgeführten Aufgaben und dem per Vorschrift verantwortlichen Mitarbeiter. Aufsichtsbehörden erstellen Anforderungen oft mit großer Verspätung und veröffentlichen sie erst dann, wenn die Technologie bereits ausgereift ist. Dieser Umstand kann Ihre etablierte Software-Roboter-Infrastruktur über Nacht obsolet machen und viel Geld kosten.

Wenn Sie nicht in der Lage sind, Aufsichtsbehörden mit Software-Robotern erstellte Ergebnisse zu erklären, kann das Geldbußen oder sogar den Verlust der Lizenz für den Markt bedeuten.

09

Rufschädigung

SZENARIO:

Online-Nachrichtenportale haben vor Kurzem eine Kampagne gegen Ihr Unternehmen gestartet, die auf von Journalisten ermittelten Kreditraten basiert. So hat ein unabhängiger Blogger einen engen Zusammenhang zwischen diesen Raten und der Hautfarbe des Kreditnehmers festgestellt. Sie wissen aber sicher, dass keine solche Entscheidung bei der Preisgestaltung getroffen wurde. Tatsächlich ist es so, dass Kreditanträge von neuen kognitiven RPA-Programmen automatisch bearbeitet und bepreist werden – Sie können nicht genau sagen, wie die Berechnung erfolgt.

BEDROHUNGSDETAILS:

Algorithmen des maschinellen Lernens können selbstständig Muster erkennen oder Entscheidungen treffen, die aus ethischer Sicht inakzeptabel sind. Das gilt besonders für multinationale Unternehmen. Der Umgang mit verschiedenen Kulturen kann sich als schwierig erweisen, selbst wenn es geeignete Testverfahren für ethnische Unterschiede gibt. Die Tester kennen möglicherweise nicht alle potenziellen Besonderheiten eines bestimmten Kulturkreises. Das kann unter gewissen Umständen den Ruf der Firma schädigen.

In einem berühmten Fall hat ein Uber-Algorithmus den Fahrpreis während der Terroranschläge in London deutlich erhöht, was zu einem riesigen Medienskandal für das Unternehmen führte.

Algorithmen des maschinellen Lernens können selbstständig Muster erkennen oder Entscheidungen treffen, die aus ethischer Sicht inakzeptabel sind.

10

Unzureichender Datenschutz

T 0.19 Offenlegung vertraulicher Daten

SZENARIO:

Kunden einer Bank kontaktierten ihre Kundenbetreuer und beschwerten sich über einen falschen Kontoauszug, den sie per E-Mail im letzten Verteileraussand erhalten hatten. Da es sich hier um Auszüge anderer Kunden der Bank handelte, machten sich die Betroffenen verständlicherweise Sorgen über die Vertraulichkeit ihrer Daten und ihre personenbezogenen Informationen. Deshalb forderten sie eine Bestätigung von der Bank, dass keine vertraulichen Daten ihrer Konten verraten wurden. Später stellte sich heraus, dass der für die Versendung der Kontoauszüge zuständige Roboter für den Fehler verantwortlich war.

BEDROHUNGSDETAILS:

Bei der Automatisierung von Aktivitäten sollte in Hinsicht auf die vertraulichen Daten unbedingt die RPA-Geschwindigkeit und -Skalierbarkeit in Betracht gezogen werden. Bei einer manuellen Ausführung besteht die Möglichkeit, dass der Fehler noch rechtzeitig erkannt wird. Bei Robotern läuten in solchen Fällen keine Alarmglocken.

Datenschutzverletzungen können sich in manchen Fällen negativ auf ein Unternehmen auswirken. Deshalb empfiehlt es sich, zusätzliche Kontrollinstanzen in den Workflow einzubetten, um die Risiken zu minimieren.

Bei ineffizienten Kontrollen kann der RPA-Einsatz zu einer unbeabsichtigten Offenlegung von vertraulichen Daten führen.

Fazit

Bei der Entstehung dieses Dokuments lagen keine öffentlichen Daten für Schwachstellen bei RPA-Software oder Berichte über Vorfälle vor, bei denen speziell diese Technologie das Ziel von Angriffen war. Trotzdem deutet die in diesem Whitepaper enthaltene Liste potenzieller Bedrohungen darauf hin, dass RPA-Risiken mithilfe eines proaktiven Ansatzes bewertet und gehandhabt werden sollten.

Die gute Nachricht für Firmen mit einem soliden ISMS: Die meisten Kontrollen für diese neue Asset-Art sind bereits integriert und erfordern nur geringe Anpassungen. In allen anderen Fällen bringen Software-Roboter eine Zunahme der Schatten-IT und ungewisse Zukunftsaussichten.

ES FOLGEN EINIGE EMPFEHLUNGEN FÜR DIE RPA-IMPLEMENTIERUNG IN IHR UNTERNEHMEN:

Richten Sie eine Arbeitsgruppe ein, die den Projektumfang, die Prozesse der RPA-Installation sowie die Geschäftsrisiken definiert.

Stellen Sie sicher, dass bei Mitarbeitern, die für die RPA-Implementierung zuständig sind, keine Interessenkonflikte vorliegen.

Entscheiden Sie, ob die RPA-Entwicklung von Drittanbietern oder internen Kräften durchgeführt wird und geschäftlichen Benutzern offensteht.

Prüfen Sie, ob Ihr Unternehmen für kognitive RPA bereit ist – oder ob es nur einfacher gestrickte Software-Roboter sein sollen.

Richten Sie eine serviceorientierte Architektur für die RPA-Technologie ein.

Passen Sie die ISMS-Richtlinien (Information Security Management System) an, um RPA-Besonderheiten zu berücksichtigen.

Achten Sie darauf, dass die RPA-Anforderungen bei den technischen Standards eine Rolle spielen.

Aktualisieren Sie Ihre IS-/IT-Kontroll- und -Risikomanagement-Frameworks mit aktuellen RPA-Richtlinien.

Beachten Sie, dass Software-Roboter nur eine von vielen neuen Technologien wie etwa Blockchain oder Internet of Things sind. Ihr ISMS muss flexibel und in der Lage sein, das Onboarding neuer Asset-Klassen schnell und effizient bewerkstelligen zu können. Auf diese Weise haben Sie Ihre Risiken im Griff und können sich auf dem Markt dank einer beschleunigten Implementierung innovativer Technologien Wettbewerbsvorteile verschaffen.

Kontaktieren Sie uns und erfahren Sie, wie ELEKS Sie mit einem ISMS unterstützen kann.

eleks

eleks

Ihr Technologie-Partner für Software-Innovationen und marktführende Lösungen

ÜBER ELEKS

Wir bieten Hightech-Innovationen für Fortune-500-Firmen, Großunternehmen und Technologieanbieter, verbessern ihre Arbeitsweise und steigern den Wert, den sie für die moderne Welt schaffen.

Unsere mehr als 1.200 Fachkräfte in Zentren in ganz Osteuropa sowie Vertriebsbüros in Europa, den USA und Japan stellen unseren Kunden eine komplette Reihe an Software-Services zur Verfügung. Dazu gehören unter anderem Datenwissenschaft, Qualitätssicherung, UX/UI, Forschung und Entwicklung, Internet of Things, Produktentwicklung sowie Technologieberatung.

ÜBER DEN AUTOR

Oleksandr Pluzhnikov – Information Security Manager mit über zehn Jahren Erfahrung in den Bereichen Cybersicherheit, Technologie und Führung in multinationalen Organisationen. Ein strategischer Denker mit fundierten Kenntnissen bei der ISMS-Entwicklung (Information Security Management System) und der Implementierung internationaler Standards für Informationssicherheit (ISO27001/2, NIST).

Weitere Informationen finden Sie unter www.eleks.com