eraneos

E-Paper

Sicherheit im IoT – Ein Thema in Bewegung

Einleitung

Das Internet of Things (IoT) steht für die zunehmende Vernetzung von virtuellen und physischen Objekten. Mit der Adaption des IoT zur Erweiterung und Optimierung von Geschäftsprozessen müssen Überlegungen zu Infrastruktur, Sicherheitsrisiken und Schutzmassnahmen angestellt werden. Nur so kann ein sicherer und gewinnbringender Einsatz mit den damit verbundenen Technologien gewährleistet werden.
In dieser Publikation werden im ersten Abschnitt typische Anwendungsfälle des IoT aufgezeigt. Im zweiten Teil werden dann die wichtigsten Punkte, die für einen sicheren Einsatz des IoT zu beachten sind, erläutert.

Benedict Simlinger
Managing Consultant, Energie- & Versorgungsunternehmen

Manuel Gantner
Manager, IoT & Control Systems

© Alle Urheber- und Veröffentlichungsrechte sind **vorbehalten;** eine Vervielfältigung oder Weitergabe an Online-Dienste, auch auszugsweise, ist nur mit Zustimmung zulässig.

Was ist das IoT?

Waren bisher Server und Computer die überwiegenden Teilnehmenden am Internet, so erweitert die Anbindung zusätzlicher Hardware wie Sensoren, Steuercomputer von Fahrzeugen, sowie Maschinen und Gebäude das herkömmliche Internet um das Internet of Things (IoT). Neben bewährten Standards und Infrastrukturen wie Internet, Mobilfunknetz, Bluetooth und Near Field Communication (NFC) bilden Ad-hoc-Mesh-Netzwerke und Low-Power-WAN-Technologien wie LoRa oder Narrowband IoT die Kommunikationsgrundlage für das IoT. Das IoT zeichnet sich im Allgemeinen durch hochspezialisierte, heterogene Hardware und Software aus, welche für einen bestimmten Zweck optimiert ist und potenziell ausserhalb der sicheren und kontrollierten Perimeter eines Firmennetzwerks kommuniziert. Parallel dazu entwickeln sich Services zur Wartung und Bedienung dieser Geräte sowie Services zur Steigerung der Wertschöpfung in Geschäftsprozessen (Abbildung 1).

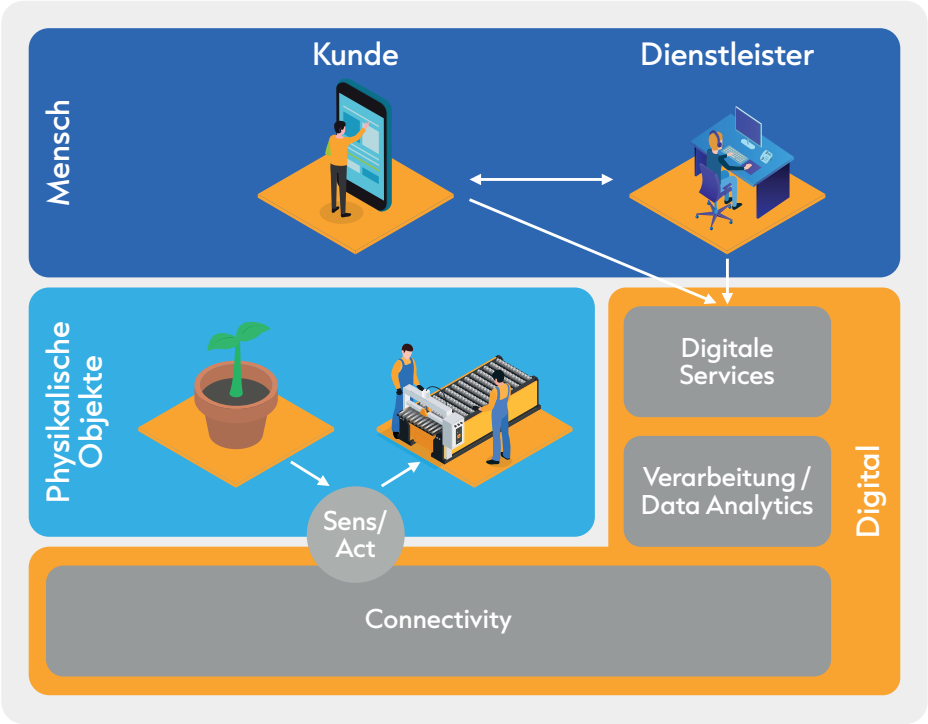


Abbildung 1: Der Einsatz von IoT umfasst mehr als die Erschliessung bisher nicht vernetzter Geräte. Zugehörige Services und Interfaces helfen, das IoT nutzbar machen.

Anwendungs-fälle IoT

Die Anwendungsgebiete des IoT und die damit verbundenen Anforderungen sind so vielfältig wie die Branchen, Produkte und Services der Unternehmen, die das IoT einsetzen. Vor diesem Hintergrund ist eine Retrospektive auf die gewonnenen Erfahrungen angebracht, um die richtigen Schlussfolgerungen zu ziehen und daraus abgeleitete Strategien vorteilhaft umzusetzen. Die nachfolgenden Anwendungsfälle bieten lediglich einen kleinen Einblick in die grosse Welt des IoT.

Flottenmanagement, Verkehr und Smart-Tools

Vor allem bei mobilen Anwendungen im Transport- und Speditionswesen und bei geographisch weit verteilten Systemen, wie sie im Städtebau und im Verkehrswesen üblich sind, überbrückt das IoT zuverlässig die Infrastruktur-Lücke. Dazu zählen eingeschränkte Energieversorgung, lückenhafte Kommunikation beziehungsweise Verfügbarkeit, schwierige Umweltbedingungen und die geteilte Verantwortung für Geräte und Infrastruktur. IoT-Lösungen ermöglichen hier eine effiziente und reibungsfreie Verwaltung von Fahrzeugflotten, bieten Mitarbeitenden im Aussendienst einfache Arbeitsinterfaces oder versorgen ein zentrales System mit Informationen zur Einsatzabwicklung.

Im IoT kommen die unterschiedlichsten Systeme zum Einsatz. Zum einen wären da Sensoren für einfache Messungen, die mit möglichst wenig Energie einmal täglich opportunistisch über ein Low-Power-WAN übertragen werden. Konkrete Anwendungsfälle sind unter anderem Aufzeichnungen der Luftqualität, das Erfassen von entnommenen Defibrillatoren oder Feuerlöschern sowie die Anzeige von freien Autoparkplätzen. Zum anderen zählen aber auch medizinische und industrielle Geräte mit hohen Anforderungen an Bedienbarkeit, Ausfallsicherheit und Echtzeitkommunikation oder Verkehrskameras mit Bildauswertung sowie entsprechend hohem Bedarf an Datenbandbreite und Zugriffschutz dazu.

Das Konzept des IoT ist auch für Zulieferer von komplexen Systemen, Maschinen oder Werkzeugen sinnvoll[1]). Durch den direkten Informationsfluss kann der Zulieferer mehr über sein Produkt und dessen Anwendung im Feld erfahren und mittels Predictive Maintenance oder Produktverbesserungen einen direkten Vorteil für den Kunden schaffen.

Spannungsfeld zwischen OT und IoT

In der Fertigungsindustrie wurden viele IoT-Feldversuche gestartet[2]). Unabhängig vom IoT nimmt im Industriegewerbe die Bedeutung der Datenverarbeitung zu. Software bietet eine Flexibilität, die mit Hardware allein kaum erreicht werden kann und ermöglicht modulare Maschinensysteme und Produktdiversifikation mit geringem Mehraufwand. Zudem erhöhen die zunehmend schnellere Auftragsabwicklung und komplexere Sensoren das Volumen der anfallenden Daten, die verarbeitet werden müssen, damit eine Maschine wettbewerbsfähig ist. All diese Parallelen zum IoT lassen ein Näheverhältnis vermuten, aus dem sich Synergien ergeben können.

1 https://www.elektronikpraxis.vogel.de/mit-intelligenten-iot-werkzeugen-den-fertigungsprozess-verbessern-a-531004/

2 In diesem Artikel wird IoT und Industrial IoT (IIoT) synonym verwendet. Eine Unterscheidung der zwei Begriffe würde über den Rahmen dieses Artikels hinausgehen.

Gleichzeitig hat die klassische OT der Industrie aber sehr unterschiedliche Anforderungen und Systemkonzepte, die in direktem Widerspruch zum IoT stehen, wie Abbildung 2 aufzeigt.

Diese Unterschiede verdeutlichen, dass eine direkte Vernetzung von OT und IoT konzeptionelle Differenzen birgt, deren Bewältigung explizite Planung und zusätzliche Infrastruktur wie zum Beispiel Edge Gateways oder Broker benötigen kann. Hier bewährt sich eine bewusste Koexistenz, in der das IoT beispielsweise die Abläufe rund um die OT unterstützt. Beispiele hierfür wären Track & Tracing-Anwendungen von erzeugten Endprodukten. Viele Hersteller haben klassische OT-Devices mit standardisierten Protokollen und Cloud-Integration erweitert und ermöglichen dadurch einen direkten Einstieg in das IoT.

Es hängt vom Anwendungsfall ab

Die vorherigen Beispiele zeigen das breite Spektrum an IoT-Anwendungsfällen auf. Die Vernetzung der Geräte und Services sowie das erweiterte Einsatzgebiet bringen viele Vorteile, aber auch grössere Verantwortung mit sich. Ganz gleich wie der Anwendungsfall aussieht, allen IoT-Anwendungen ist eines gemeinsam: Die Sicherheit der Geräte, Kommunikationswege und Daten muss den Anforderungen entsprechend gewährleistet werden. Nachfolgend werden entsprechende Sicherheitsrisiken und -ziele sowie Bewältigungsmassnahmen aufgezeigt[3]).

OT	IoT
Daten innerhalb des Netzwerksegments verfügbar	Daten netzwerkübergreifend verfügbar
Wenige, teure Maschinen	Viele, kleine, günstige Devices
Hohe Verfügbarkeit	Verfügbarkeit stark variabel
Hohe Anschaffungskosten	Vergleichsweise geringe Anschaffungskosten
Echtzeitkommunikation	Echtzeitfähigkeit nur teilweise gegeben
Hierarchisch organisiert	Mesh-Organisation
Bedienung nur durch ausgebildetes Personal	Unbewusste Nutzung oder bedienbar für Laien

3 https://csrc.nist.gov/publications/detail/nistir/8228/final

Abbildung 2: Gegenüberstellung von Merkmalen der OT und IoT Infrastruktur.

Sicherheits-risiken des IoT

Physische Interaktion

Geräte im IoT interagieren mit der physischen Welt in einem Ausmass, wie es bisher nur in wenigen Industrien aus der OT bekannt war. Sensoren und Aktoren werden in einer Umgebung eingesetzt, die oft nicht so kontrolliert und sicher ist wie eine Fabrikhalle, sondern im Gegenteil sogar als nicht vertrauenswürdig eingestuft werden muss. Sie steuern Systeme wie zum Beispiel Fahrzeuge, Beleuchtung oder Kühlsysteme, die als Teil eines grösseren Systems Ereignisketten mit ernsten, unumkehrbaren Folgen auslösen können.

Durch die gleichzeitige Vernetzung und Anbindung an IT-Systeme bilden IoT-Systeme eine bidirektionale Brücke zwischen der physischen Welt und der Software, die bestmöglich geschützt werden muss.

Schwer zu managen

Obwohl IoT-Geräte dem Endanwender Arbeitsvorgänge erleichtern oder ganz abnehmen (z.B. die Inventur), benötigt zusätzliche Hardware immer den Auf- oder Ausbau einer entsprechenden Verwaltungsinfrastruktur samt Schulungen der Mitarbeitenden. Im Vergleich zu IT- oder Industrieanwendungen kommt hier aber erschwerend hinzu, dass IoT-Geräte oft nur schwer wartbar sind. Sie sind oft nicht physisch verfügbar, benötigen heterogene Verwaltungstools, sind nicht lückenlos überwachbar oder das nötige Bewusstsein beziehungsweise Know-how fehlt. Besonders dem letzten Punkt muss bei langlebigen IoT-Geräten mit einer nachhaltigen Strategie entgegengewirkt werden.

Begrenzte Sicherheitsfunktionen

IoT-Geräte sind in der Regel stark spezialisierte Hardware mit ebenso spezialisierter Software, um den hohen Anforderungen an Energieverbrauch, Kosten und Widerstandsfähigkeit gerecht zu werden. Unter diesen Umständen bleiben kaum Ressourcen für sekundäre Funktionen, wie zum Beispiel Update-Mechanismen, die nichts mit dem primären Verwendungszweck zu tun haben. Wer diesen Aspekt während der Planung und Beschaffung nicht beachtet, hält mögliche Einfallstore bewusst offen und setzt sich mit zunehmender Zeit einem gesteigerten Risiko aus.

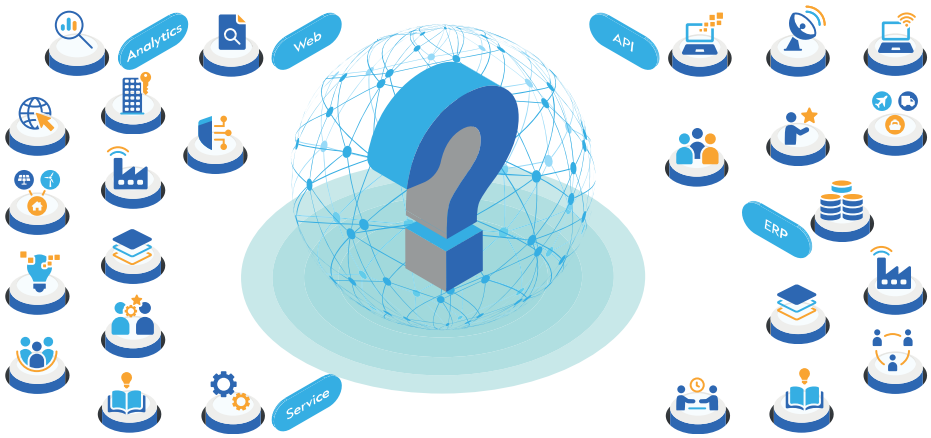


Abbildung 3: Die zunehmende Vernetzung von Sensoren, Maschinen und Computern stellt die Unternehmen in Bezug auf ihre Sicherheitsstrategie vor neue Herausforderungen.

Sicherheits-ziele

Das Management der oben genannten Sicherheitsrisiken kann durch eine Kombination aufeinander aufbauender Sicherheitsziele erreicht werden (Abbildung 4).

Device Security

Das IoT-Gerät selbst sowie auch die Infrastruktur müssen abgesichert werden. Das gilt für Hardware, Software (Sicherheitslücken) und Fehler beziehungsweise Nachlässigkeit in der Konfiguration, wobei letzteres in der Regel der zuverlässigste Vektor für Angreifende ist[4]). Nur so kann vermieden werden, dass ein IoT-Gerät selbst zum Einfallstor für Angriffe auf weitere Geräte im gleichen Netzsegment wird, wie es bei „Ripple 20"[5]) passiert ist.

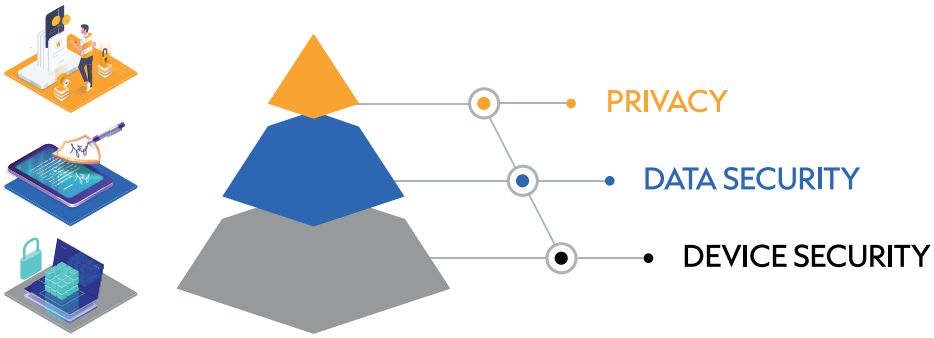
Folgende Aspekte (und die dazugehörigen Prozesse im Unternehmen) müssen hier beachtet werden:

- Geräte- und Softwareverwaltung für den regulären Betrieb
- Schwachstellenmanagement
- Zugriffs- und Berechtigungsmanagement
- Erkennung von Vorfällen und Logging

Software-Updates

Update-Mechanismen kosten Ressourcen und sind Teil der Angriffsfläche. Zertifikate und Firmware können eventuell gar nicht online erneuert werden und benötigen Betriebsroutinen mit physischem Zugriff auf das Gerät. Vor allem in mobilen Anwendungen kann es so zu grossen Verzögerungen und Kosten durch Update-Prozesse kommen. Daher ist es zwingend notwendig, Prozesse, Kompetenzen und Verantwortung im Unternehmen zu etablieren, bevor IoT-Geräte und die zugehörige Infrastruktur in Betrieb genommen werden.

Besonders bei IoT-Geräten von Drittanbietern ist die zukünftige Versorgung mit Software-Patches vom Hersteller für den geplanten Life Cycle zu sichern[6]). Sofern externe Infrastruktur benötigt wird (z.B. Command-and-Control-Server), ist diese Abhängigkeit zu berücksichtigen. Ein weit sichtbares



4 https://labs.bishopfox.com/tech-blog/breaking-https-in-the-iot

5 https://www.heise.de/security/meldung/Ripple20-erschuettert-das-Internet-der-Dinge-4786249.html

6 Gerätesicherheit über die Supply Chain durchzusetzen ist ein bekanntes Konzept, aber nach wie vor kaum standardisiert. https://www.schneier.com/blog/archives/2020/07/securing_the_in_1.html

Abbildung 4: Die Sicherheitsziele bauen aufeinander auf. Ohne Sicherung des Geräts selbst können auch die Daten auf diesem Gerät nicht gesichert werden.

Beispiel, das eher Konsumenten statt Unternehmen getroffen hat, ist die „Philips Hue Bridge", welche im Q1 2020 von Philips abgekündigt wurde[7]), für die aber nach wie vor neue Exploits rauskommen[8]). Hier stellen IoT-Geräte nicht nur eine Gefahr für sich selbst dar, sondern gefährden das gesamte Netz.

Hardware-Lifecycle
Hardware im Business- und Industrial-Umfeld hat einen wesentlich längeren Life Cycle als Konsumentenelektronik. Gleichzeitig können IoT-Geräte allen voran im mobilen Einsatz wesentlich schwierigeren Umweltbedingungen (Temperatur, Erschütterungen, Nässe, Stromversorgung) ausgesetzt sein. Dadurch ist ein stringentes Gerätemanagement notwendig, sodass zum Beispiel Module im Rahmen der Predictive Maintenance mit geringem Aufwand getauscht werden können, ehe es zu teuren Ausfällen im Feld kommt.

Data Security

Ist das Gerät gesichert, müssen als Nächstes die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der übertragenen Daten gesichert werden. Diese Anforderungen müssen beim Sammeln, Speichern, Verarbeiten und Übertragen der Daten erfüllt sein.

Mit zusätzlichen Daten und Systemkomponenten geht zusätzliche Verantwortung einher. Es ist Teil der Sorgfaltspflicht, ein stimmiges und robustes Datenkonzept zu erarbeiten und umzusetzen. In diesem Konzept sollte stehen, welches Problem gelöst werden soll, wo die Daten zur Lösung erhoben werden sollen, wie die Daten weiterverarbeitet und gelagert werden sollen, und wann sie wieder gelöscht werden. Bei diesen Fragen gilt: Weniger ist mehr. Das wird langfristig Aufwand und eventuell sogar juristisches Kopfzerbrechen ersparen[9]).

In Anbetracht der absehbaren Verschärfung der regulatorischen Anforderungen an die IoT-Sicherheit in der Schweiz[10]) und der EU (z.B. bei der Zulassung von Fahrzeugen[11]) ab 2022 beziehungsweise 2024) ist die Investition in ein vorausschauendes Datenschutzkonzept eine sinnvolle Geschäftsentscheidung.

Privacy

Sofern personenbezogene Daten verarbeitet werden, müssen das Schweizer Datenschutzgesetz oder entsprechende Richtlinien wie die DSGVO umgesetzt werden. Dazu gehören die Anonymisierung der Daten und die Aufklärung der Nutzer sowie Techniken zur Erkennung von Datenverlust.

7 https://www2.meethue.com/en-us/support/end-of-support-policy

8 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6007

9 https://www.latimes.com/business/story/2020-02-24/autopilot-data-secrecyt

10 https://www.inside-it.ch/de/post/bundesrat-will-mehr-sicherheit-im-internet-der-dinge-20200429

11 https://undocs.org/ECE/TRANS/WP.29/2020/79

Bewältigungs-massnahmen

Risiken und Herausforderungen kennen

Eine gründliche Erarbeitung und Bewertung der Sicherheitsrisiken, wie sie in diesem Artikel zuvor skizziert wurden, mitsamt der Definition der zugehörigen Sicherheitsziele ist der Grundstein für die erfolgreiche Umsetzung der Sicherheitsstrategie. Essenziell ist hier ein offener und ehrlicher Umgang mit Unbekanntem. Anstatt sich darüber auszuschweigen und damit Lücken (konzeptioneller wie auch technischer Natur) zu unterschlagen, müssen diese explizit dokumentiert werden. Nur so ist eine echte Chance auf gezielte Verbesserung gegeben. Ein einfacher Katalog offener Fragen ist bereits ein sinnvoller erster Schritt:

- Welche Geräte sind IoT-Geräte und in den bestehenden IT-Richtlinien unzureichend erfasst?
- Gibt es eine stets aktuelle und vollständige Liste dieser Geräte? Wer ist hier verantwortlich beziehungsweise Wissensträger?
- Welche Dokumente bestehen bereits (Risikobewertung, Schutzkonzept, Anleitungen), wer ist verantwortlich und wann werden diese das nächste Mal aktualisiert?
- Auf welche Weise kann mit den Geräten kommuniziert werden (das schliesst Hardwareschnittstellen ein)?
- Wer hat Zugriff auf die Geräte und wie wird diese Person authentifiziert?
- Wie werden die Firmware- und Software-Updates der Geräte aktuell geplant und durchgeführt? Wie wird die Verfügbarkeit von Updates geprüft?
- Welche Daten werden gesammelt, wo werden sie gespeichert und wohin werden sie transferiert?
- Wie wird ein Ausfall und/oder Verlust eines Geräts festgestellt und welche Aktionen folgen darauf?

Diese Frageliste berührt alle Bereiche eines stimmigen Sicherheitskonzepts, ist aber nicht abschliessend. Nutzen Sie die Fragen, um den Zustand Ihres aktuellen Schutzkonzepts zu prüfen.

Unternehmensregeln und Prozesse anpassen

Verantwortungsbereiche und Prozesse im Zusammenhang mit IoT Security müssen klar und akzeptiert sein. Die Verantwortlichen müssen insbesondere die Berechtigungen, Kompetenzen und Ressourcen haben, um ihre Verantwortung wahrzunehmen.

Weiter muss der Geltungsbereich und insbesondere die Geltungsdauer der Sicherheitsrichtlinien eindeutig definiert sein. Das bedeutet, dass klar nachvollziehbar ist, welche Geräte als IoT-Geräte gelten und wie sich diese Klassifikation ergibt.

Aus den Unternehmensregeln muss ersichtlich sein, welche Risken akzeptiert, vermieden, gemindert, geteilt oder auf andere übertragen werden und wie die zugehörigen Prozesse gestaltet sind.

Bestehende Bestimmungen und Dokumente müssen regelmässig entsprechend angepasst werden.

Implementieren und wiederholen

Durch den stetigen Wandel der Technik müssen die IoT-Sicherheitsmassnahmen periodisch auf ihre Zulänglichkeit geprüft werden. Gleichzeitig werden auch die eingeführten Änderungen validiert. Sofern Handlungsbedarf ersichtlich wird, sind Risiken und Herausforderungen neu zu bewerten und die entsprechenden Sicherheitsmassnahmen in Form von Regeln und Prozessen bis zur nächsten periodischen Prüfung umzusetzen.

Fazit

Die zunehmende Vernetzung von Geräten und Maschinen kann Unternehmen Chancen und Wettbewerbsvorteile bieten. Um diese Vorteile nachhaltig sicherzustellen ist es notwendig, die Verantwortung und Herausforderungen in der Geräte- und Datensicherheit wahrzunehmen und proaktiv anzugehen.

eraneos

Experienced in a wide range of industries

Eraneos Group ist eine internationale Management- & Technologieberatungsgruppe, die Dienstleistungen von Strategie bis Implementierung anbietet. Sie ist aus dem 2021 angekündigten Zusammenschluss von Ginkgo Management Consulting, Quint Group und AWK Group hervorgegangen. Die Gruppe betreut Kunden auf drei Kontinenten, wo rund 1.000 engagierte und hochqualifizierte Fachleute gemeinsam daran arbeiten, das volle Potenzial der Digitalisierung auszuschöpfen. Die Dienstleistungen reichen von der Entwicklung digitaler Geschäftsmodelle und Datenanalysen bis hin zu Cybersicherheit, von Sourcing und IT-Beratung zum Management komplexer Transformationsprojekte. Eraneos Group hat Niederlassungen in der Schweiz, Deutschland, Luxemburg, Spanien, den Niederlanden, China, Singapur und den USA. 2021 erzielte die Gruppe einen Umsatz von fast 200 Millionen Euro.

Contact us >

Our offices >

Visit our website >