

se cu. rity

Paving
the way to
security



TÜV NORD GROUP Kurzprofil

Die TÜV NORD GROUP ist ein weltweit tätiger Technologiedienstleister und steht für höchste Ansprüche bei Sicherheit, Unabhängigkeit und Qualität. Seit mehr als 150 Jahren machen wir technologische Revolutionen für die Menschen nutzbar und sicher. Mit unseren sechs Business Units und nahezu 100 Gesellschaften innerhalb und außerhalb Deutschlands bieten wir mehr als 1.500 Dienstleistungen in den Geschäftsfeldern Testing, Inspection, Certification, Consulting, Engineering und Training an. Im persönlichen Dialog mit unseren Kundinnen und Kunden schaffen wir Vertrauen in Technologie für sichere und nachhaltige Lösungen.

TUVNORDGROUP · **TUVNORD** · **DMT** · **ALTER** · **TUVIT**

Inhalt

04 Inspired by Knowledge

10 Paving the way to security

12 KI mit System

14 Schlüssel der Zukunft

16 Schützen, was uns trägt

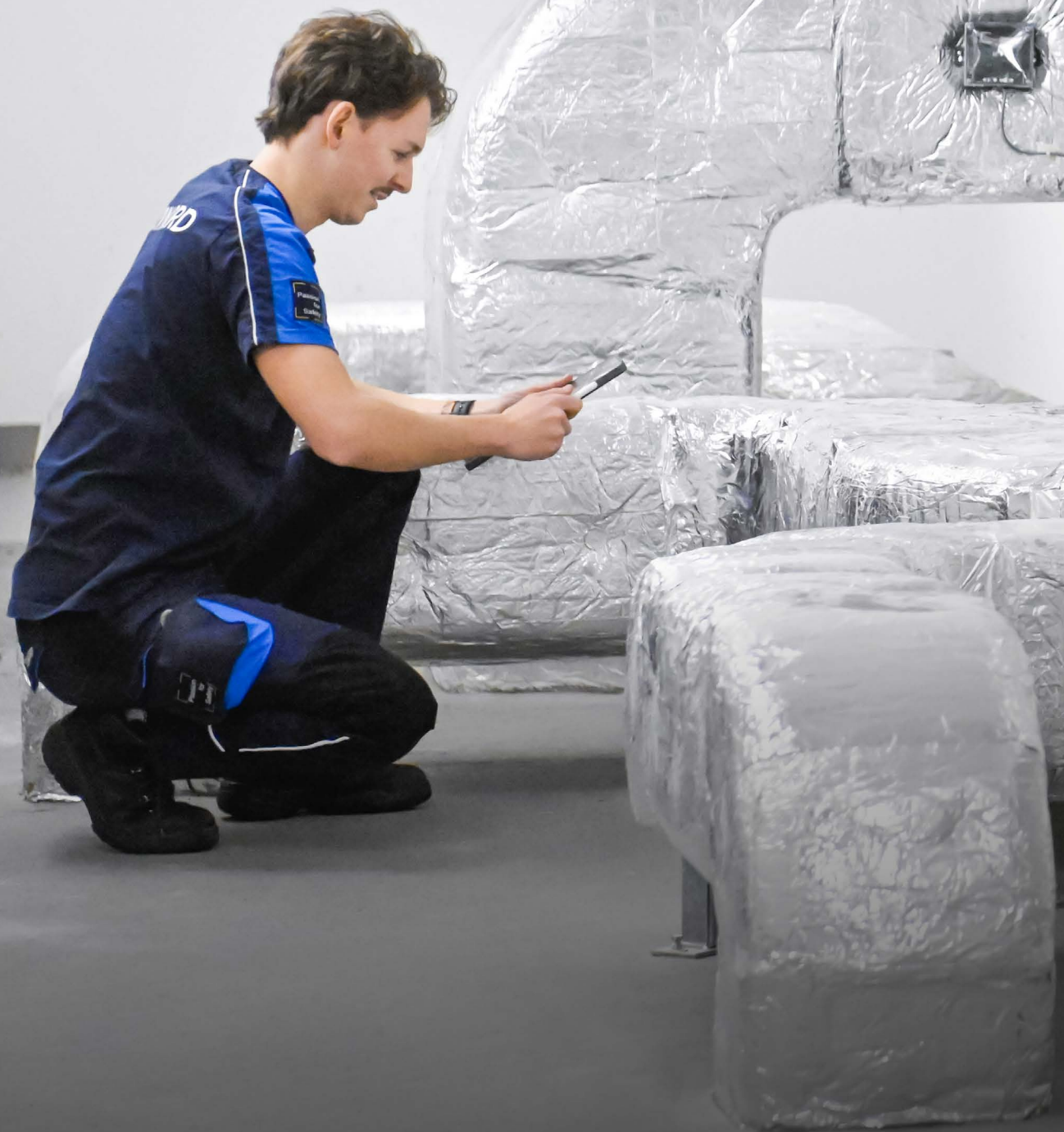
18 Mit Sicherheit smart geprüft

20 Daten-Diagnose mit Durchblick

22 Fit für den Cyberschutz

24 Digitale Transformation startet in Indonesien

30 Impressum





Digitalisierung verändert die Arbeitswelt. Gleichzeitig bietet sie viele neue Chancen. Doch sie schafft auch Abhängigkeiten von elektronischen Systemen, die immer häufiger Ziel von Angriffen werden. Mit unserer Kompetenz verhindern wir dies, schützen Systeme und sensibilisieren Menschen für diese Risiken. So unterstützen wir dabei, Geschäftsprozesse sicherer zu machen und das Bewusstsein für Bedrohungen zu schärfen.

Technologie macht immer rasantere Sprünge. Was gestern undenkbar war, ist heute schon Realität. Sicherheit und Verlässlichkeit bleiben bei allem Fortschritt entscheidende Kriterien. Hier zeigt sich unsere Kompetenz: Wir prüfen technische Geräte, zertifizieren Systeme, entwickeln neue Standards und Prüfverfahren. So ist Technik weiterhin verlässlich und vertrauenswürdig.







ALTER

Datenströme kennen keine Grenzen auf ihrer Reise um den Globus und darüber hinaus. Sie sind das Rückgrat der Wirtschaft. Weil schon kleine Störungen gravierende Auswirkungen haben können, wird unser Know-how geschätzt: Wir begleiten Hersteller dabei, Systeme sicher aufzusetzen. So entstehen robuste Infrastrukturen, die Daten schützen, Bedrohungen neutralisieren und weltweit Vertrauen schaffen.



se cu rity

Paving
the way to
security

Als TÜV NORD GROUP gestalten wir technologische Innovationen aktiv mit, indem wir sie von Grund auf gegen digitale Bedrohungen wappnen. Sechs Beispiele.



Thora Markert, Produktmanagerin für
KI bei TÜV NORD CERT



Business Unit Certification

KI mit System

Künstliche Intelligenz braucht Vertrauen: Mit der weltweit ersten Zertifizierung nach ISO/IEC 42001 schaffen TÜV UK und TÜV NORD Nederland den Standard für sicheren und verantwortungsvollen KI-Einsatz.

„Künstliche Intelligenz ist eine Technologie, die enorme Chancen bietet, aber auch viele Risiken mit sich bringt“, erklärt Thora Markert, Produktmanagerin für KI bei TÜV NORD CERT. Die Bandbreite möglicher Herausforderungen ist groß: von technischen Fehlfunktionen und Manipulationsrisiken über Angriffe auf KI-Systeme bis hin zu ethischen Fragen. „Das sind völlig neue Aspekte, die für frühere Technologien in dieser Form keine Relevanz hatten“, sagt Markert. Gerade deshalb sind Unternehmen gefordert, verantwortungsbewusst mit KI umzugehen, denn nur so lassen sich Sicherheit und Integrität ihrer Systeme sicherstellen.

Genau an diesem Punkt setzt die Norm ISO/IEC 42001 an: Sie ist der weltweit erste internationale Standard für Managementsysteme im Bereich KI. „ISO/IEC 42001 bildet einen Rahmen, um KI-Systeme verantwortungsvoll und effektiv zu implementieren, einzusetzen und Risiken einzudämmen“, erläutert Markert. „Jetzt haben TÜV UK und TÜV NORD Nederland die Akkreditierungen erhalten.“ Die Norm legt besonderen Wert auf den Schutz von Menschen und Gesellschaft, auf das Management sozialer Risiken sowie die Einhaltung ethischer, datenschutzrechtlicher und sicherheitstechnischer Anforderungen.

Die Zertifizierung nach ISO/IEC 42001 hilft Unternehmen, den wachsenden regulatorischen Anforderungen gerecht zu werden. Denn wie viele andere Weltregionen legt auch die EU derzeit rechtliche Rahmenbedingungen für KI fest. Im Sommer 2024 verabschiedete sie den EU AI Act, der bis August 2027 nach und nach hochgefahren wird. „Mit der schrittweisen Einführung des AI Acts wird die Nachfrage nach Zertifizierungen deutlich steigen“, prognostiziert Markert. Auch Unternehmen außerhalb der EU, die KI-basierte Produkte in Europa anbieten, müssen die Vorgaben des EU AI Acts erfüllen. Die Einführung der Zertifizierung erfolgte in enger Zusammenarbeit zwischen TÜV UK und TÜV NORD Nederland, die im TÜV NORD Konzern Vorreiter bei der Akkreditierung sind. TÜV NORD CERT unterstützt die beiden Auslandsgesellschaften und strebt in Zukunft ebenfalls eine entsprechende Akkreditierung an. „Gemeinsam haben wir einen effektiven Zertifizierungsprozess entwickelt, den wir auch anderen Auslandsgesellschaften zur Verfügung stellen“, sagt Markert. „Damit können wir weltweit hochwertige Zertifizierungen für KI-Systeme anbieten und Unternehmen optimal in ihren jeweiligen Märkten unterstützen.“

Business Unit Digital & Semiconductor

Schlüssel der Zukunft

TÜVIT errichtet in Essen ein hochmodernes Forschungslabor für Quantum Key Distribution (QKD)-Systeme. Dort werden die Grundlagen für die Prüfung und Zertifizierung von Systemen geschaffen, die eine sichere Datenverschlüsselung mit Quantentechnologie ermöglichen.

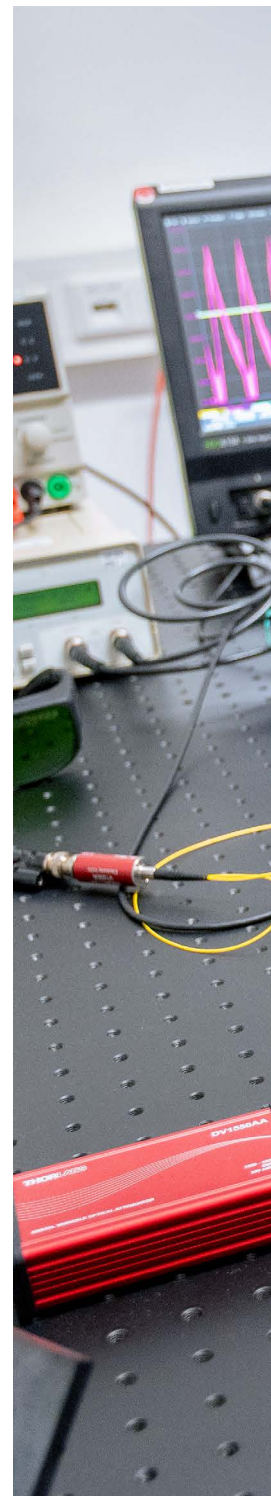
In unserer digitalen Welt gibt es immer mehr vernetzte Geräte, die zunehmend Daten erzeugen. Verschlüsselungssysteme sind enorm wichtig, um diese Daten zu schützen. Doch klassische Verfahren könnten schon bald von Quantencomputern geknackt werden. Denn diese ermöglichen mit einer neuen Art der Datenverarbeitung bisher unbekannte Rechenleistungen. „Ein gängiges Verfahren zur Datenverschlüsselung ist der sogenannte Schlüsselaustausch. Dabei werden zwei Primzahlen kombiniert, sodass eine sehr große Zahl entsteht“, erklärt Sven Bettendorf, Fachexperte für Quantentechnologie bei TÜVIT. „Ein klassischer Computer bräuchte Millionen von Jahren, um die ursprünglichen Primzahlen zurückzurechnen. Ein Quantencomputer schafft das in wenigen Minuten.“

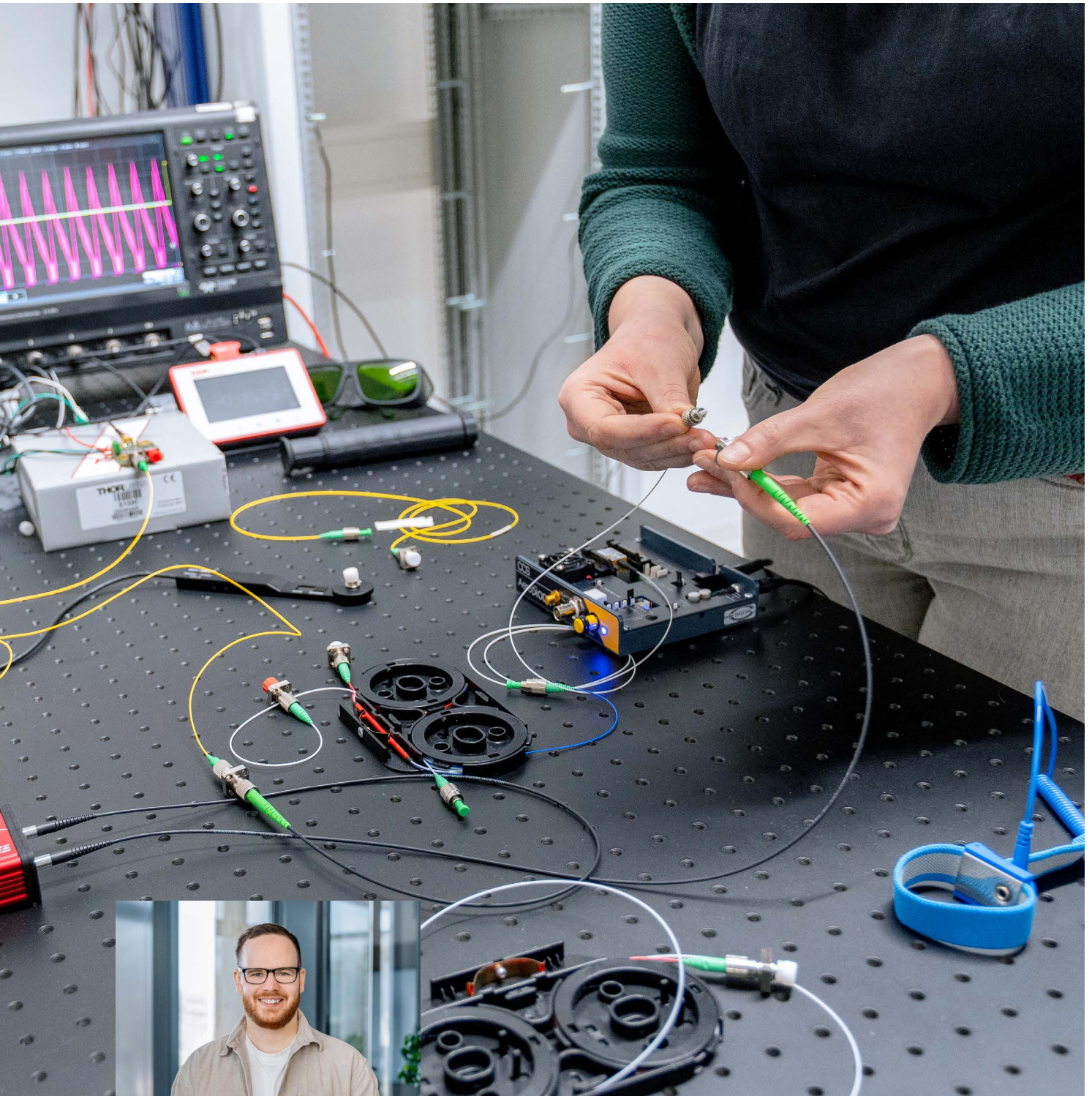
Deshalb sind neue Ansätze zur sicheren Datenverschlüsselung notwendig – wie die QKD, bei der der Schlüsselaustausch auf physikalischen Gesetzen basiert. „Damit schlägt man die Quantentechnologie mit ihren eigenen Waffen“, erklärt Bettendorf. Allerdings müssen für den praktischen Einsatz dieser Methode noch einige Hürden überwunden werden.

Ziel des neuen Forschungslabors von TÜVIT in Essen ist es, technologische Grundlagen für die Prüfung, Qualifizierung und Zertifizierung von QKD-Komponenten und -systemen zu schaffen. Die Basis dafür ist die Förderung durch das Projekt „Blueprint eines Zertifizierungs-Eco-Systems für QKD-Systeme und -anwendungen“ des Bundesministeriums für Forschung, Technologie und Raumfahrt.

„Wahrscheinlich gibt es kein Labor auf der Welt, das in diesem Bereich schon so professionell aufgestellt ist“, sagt Bettendorf. Eine Besonderheit ist das offene optische Laserlabor, in dem Forschende zentrale Gerätekomponenten gezielt mit einem Laser manipulieren und mögliche Angriffsszenarien simulieren können.

Der Aufbau des Labors wurde bereits 2025 abgeschlossen, nun beginnt die Erprobung. „Unser Ziel ist es, 2027 erste Prüfungen und Zertifizierungen durchführen zu können“, erklärt Bettendorf. Damit unterstützt TÜVIT nicht nur Hersteller von QKD-Systemen, sondern stärkt auch die Rolle der deutschen Industrie in diesem zukunftsweisenden Technologiefeld.





Sven Bettendorf, Fachexperte für
Quantentechnologie bei TÜVIT

Jan Struve, Leiter Brand- und Explosionsschutz bei TÜV NORD EnSys, und **Burkhard Rose-Mende**, Leiter Geschäftsfeld Cyber Security & Critical Infrastructures bei TÜV NORD IT Secure Communications



Business Unit Energy & Resources

Schützen, was uns trägt

Kraftwerke, Flughäfen, Wasserversorger – kritische Infrastrukturen (KRITIS) sind das Rückgrat unserer Gesellschaft. TÜV NORD EnSys und TÜV NORD IT Secure Communications vereinen jetzt ihre Expertise, um systemrelevante Einrichtungen ganzheitlich abzusichern – ein bundesweit einzigartiges Angebot.

Für Betreiber kritischer Infrastrukturen sind die Folgen eines Ausfalls gravierend. Der Druck auf diese Unternehmen steigt, denn sie müssen sich gegen grundverschiedene Gefahren wie Naturkatastrophen und Cyberangriffe wappnen. Genau hier setzt die neue Kooperation an.

Jan Struve leitet bei TÜV NORD EnSys den Bereich Brand- und Explosionsschutz. Sein Team bewertet seit Langem sicherheitstechnische Fragestellungen bezüglich Kernkraftwerken und kennt sich deshalb mit Risikotechnologien aus. Burkhard Rose-Mende verantwortet bei TÜV NORD IT Secure Communications das Geschäftsfeld Cyber Security & Critical Infrastructures. Künftig bringen beide Experten die Kompetenzen ihrer Bereiche in einem deutschlandweit einzigartigen Angebot zusammen: dem Business Continuity Management, das physische Sicherheit mit IT-Security verbindet. Gemeinsam bereiten sie Unternehmen darauf vor, bei Stromausfällen, Hackerangriffen oder Bränden den Betrieb schnell weiterführen zu können oder wiederherzustellen.

„Viele unserer Bestandskunden arbeiten mit Insellösungen – Brandschutz hier, IT-Sicherheit dort. Das verzahnen wir nun systematisch und rennen damit offene Türen ein“, erklärt Struve. Am Anfang analysiert er zusammen mit dem Kunden systematisch, welche Risiken bestehen, priorisiert sie und leitet geeignete Maßnahmen ab. Die Corona-Pandemie und der Krieg in der Ukraine hätten gezeigt, dass Unternehmen oft nicht wüssten, wo sie verwundbar sind – bis kritische Prozesse ausfallen.

Die Umsetzung der Richtlinie zur Netzwerk- und Informationssicherheit veranlasst Unternehmen zu handeln, unterstreicht Rose-Mende: „Der Geltungsbereich wird ausgeweitet, die Anforderungen verschärft.“ Die Zahl der betroffenen Unternehmen wird von derzeit etwa 4.500 auf voraussichtlich 29.500 steigen.

Die Idee zur Zusammenarbeit entstand aus der Praxis: Rechenzentren dienten als Blaupause und zeigten, wie wertvoll die Verbindung beider Disziplinen ist. Besonders vielversprechend ist der Markt der Stadtwerke, in dem beide Unternehmen bereits über etablierte Kundenbeziehungen verfügen. Mit dem integrierten Ansatz profitieren die Kunden von der gebündelten Expertise und TÜV NORD positioniert sich optimal in diesem wachsenden Markt.



Business Unit Industry

Mit Sicherheit smart geprüft

Der koreanische Elektronikhersteller Samsung hat zum ersten Mal Smart-Home-Geräte von TÜV NORD prüfen und zertifizieren lassen – und macht sich so stark für den Cyber- und Datenschutz in vernetzten Umgebungen.

Smart-Home-Produkte – wie intelligente Kühlschränke, die anhand des Vorrats eine Einkaufsliste erstellen, oder Saugroboter, die bestimmte Objekte erkennen und sich so besser orientieren – können den Alltag einfacher machen. „Ein Gerät wird zum Smart-Home-Produkt, wenn es vernetzt ist und mit seiner Umwelt interagiert“, erklärt Matthias Springer, Senior Vice President Functional Safety & Security bei TÜV NORD. Mit wachsender Vernetzung steigt jedoch auch die Verantwortung: Damit ein Gerät nicht zum Einfallstor für Hacker werden kann, müssen Hersteller ihre Produkte gegen Cyberangriffe absichern.

Der Cyber Resilience Act (CRA) legt seit 2024 in der EU Mindestanforderungen an IT-Sicherheit fest. TÜV NORD prüft und zertifiziert vernetzte Produkte für das Internet of Things (IoT) und orientiert sich dabei an der Norm ETSI EN 303 645, die einen Leitfaden zur Einhaltung des CRA enthält.

Bei der Prüfung müssen Hersteller zum einen durch Dokumentation nachweisen, dass ihre Produkte bestimmte Sicherheitsmerkmale erfüllen, zum anderen werden die Geräte selbst Verifizierungs- und Validierungstests unterzogen. „Passwortschutz, Authentifizierung und Dokumentation durch Benutzerinnen und Benutzer sind die zentralen Punkte“, sagt Kim Youngcheon, Ingenieur bei TÜV NORD Korea.

Samsung ließ erstmals zwei Serien von Saugrobotern, den Bespoke AI Jet Bot Stream und den Bespoke Jet Bot Combo sowie eine Reihe von Bespoke AI-Kühlschränken testen – mit Erfolg. Das herstellerunabhängige TÜV NORD-Prüfzeichen „Certified Cybersecurity“ soll Verbraucher:innen besseren Schutz bieten, Orientierung bei der Kaufentscheidung geben und Sicherheitsbedenken verringern.

„Wir sind sehr stolz darauf, gemeinsam mit dem Team in Deutschland die erste IoT-Zertifizierung nach ETSI EN 303 645 für Samsung durchgeführt zu haben“, freut sich Kim Soyeon, Assistant Engineering Manager bei TÜV NORD Korea. „Dieses Projekt und die Zertifizierung sind ein Meilenstein in der IoT-Cybersicherheit und werden neue Maßstäbe für den Markt setzen.“

Ende 2027 endet die Übergangsphase des CRA; bis dahin werden die Anforderungen schrittweise verschärft. „Wir werden mit den Regulierungen mitgehen und unsere Kunden auch in Zukunft mit unserer Expertise unterstützen“, sagt Springer. Wichtig sei nun vor allem, die Kunden zu informieren und für die kommenden Vorschriften zu sensibilisieren.





Matthias Springer, Senior Vice President Functional Safety & Security bei TÜV NORD, **Kim Youngcheon**, Ingenieur bei TÜV NORD Korea, und **Kim Soyeon**, Assistant Engineering Manager bei TÜV NORD Korea





Gero Eggers, Produktentwickler und Produktmanager bei TÜV NORD Mobilität

Business Unit Mobility

Daten-Diagnose mit Durchblick

Mit der TÜV NORD Onboard Car Diagnosis kommt eine innovative Lösung in moderne Fahrzeuge, die digitale Inspektionen sicherer, effizienter und transparenter macht – und Potenzial für weitere Anwendungsfelder bietet.

Moderne Pkw sind längst mehr als nur Fortbewegungsmittel – sie sind rollende Datenspeicher. Von Navigationszielen über Anruflisten bis hin zu Zahlungsdaten sammeln sie im Lauf der Zeit enorme Mengen sensibler Daten, vor allem über die Verbindung mit dem Smartphone. Damit unterliegen auch Fahrzeuge den steigenden regulatorischen Anforderungen an die digitale Informationssicherheit.

Ein Risiko entsteht vor allem dann, wenn ein Auto die Besitzerin oder den Besitzer wechselt. „Es gibt viele Szenarien, in denen es kritisch ist, wenn bestimmte Informationen noch im Fahrzeug gespeichert sind“, weiß Gero Eggers, Produktentwickler und Produktmanager bei TÜV NORD Mobilität.

Doch dabei geht es nicht nur um ungeschützte Daten, sondern auch um manipulierte Kilometerstände oder verschleierte Fehler. Genau hier setzt die TÜV NORD Onboard Car Diagnosis an. Das System wird über die On-Board-Diagnose-Schnittstelle mit dem Fahrzeug verbunden und liefert innerhalb weniger Minuten eine umfassende Analyse. Als „One-Dongle-Lösung“ vereint es mehrere Dienstleistungen: Persönliche Informationen werden (angeleitet via App) DSGVO-konform bereinigt, technische Probleme über die Fehlerspeicheranalyse sichtbar gemacht und Kilometerstand sowie Fahrzeug-Identifikationsnummer auf Plausibilität geprüft. Für diese innovative Lösung wurde das System für den Best of Industry Award 2025 im Bereich Automotive in der Kategorie „Elektrik/Elektronik & Software“ als eine der Top-3-Innovationen ausgezeichnet. „Es ist erstaunlich, wie viele Fahrzeuge tatsächlich manipuliert sind“, berichtet Eggers. Die TÜV NORD Onboard Car Diagnosis erkennt, auf welchen Steuergeräten Kilometerstände und Identifizierungsnummern gespeichert sind, und deckt Abweichungen zuverlässig auf. Auch eine „falsche Identität“ eingebauter Ersatzteile lässt sich so nachvollziehen.

Darüber hinaus eröffnet die Lösung weitere Perspektiven. „Wir haben viele Ideen für zusätzliche Anwendungen – für unterschiedliche Dienstleistungen, Kundengruppen und Fahrzeugtypen“, erklärt Eggers. Die neueste Erweiterung ist ein Batteriecheck für E-Fahrzeuge, mit dem sich der Zustand der Antriebsbatterie zuverlässig beurteilen lässt. Alle erfassten Daten werden anonymisiert und auf sicheren Servern gespeichert. Damit erfüllt die TÜV NORD Onboard Car Diagnosis nicht nur aktuelle Datenschutzerfordernisse, sondern schafft auch die Basis für weitergehende Analysen. „Langfristig lässt sich dieser Datenpool auswerten und für mehr Sicherheit im Straßenverkehr nutzen“, so Eggers.

Business Unit People & Empowerment

Fit für den Cyberschutz

Cybersicherheit betrifft längst nicht mehr nur Großkonzerne – auch mittelständische Unternehmen geraten zunehmend ins Visier von Hackern. Mit der NIS-2-Expertenschulung der TÜV NORD Akademie machen sich Unternehmen gezielt widerstandsfähig und erfüllen die neuen gesetzlichen Vorgaben.

Die Bedrohungslage durch Cyberangriffe wächst mit fortschreitender Digitalisierung. Deshalb hat die Europäische Union die Richtlinie für Netz- und Informationssicherheit grundlegend überarbeitet. „Die Anforderungen wurden extrem verschärft“, erklärt Melanie Braunschweig, Produktmanagerin bei der TÜV NORD Akademie. Die neue NIS-2-Richtlinie (EU) 2022/2555 verpflichtet künftig nicht nur Betreiber kritischer Infrastrukturen, sondern auch zahlreiche mittlere und große Unternehmen aus weiteren Sektoren zur Umsetzung strengerer Standards in der Cyberresilienz. Darauf hat die TÜV NORD Akademie frühzeitig reagiert. „Dank genauer Marktbeobachtung und offener Kommunikation konnten wir als Vorreiter ein passgenaues Schulungsangebot entwickeln“, so Braunschweig.

Rund 30.000 Unternehmen aus 18 Sektoren wie digitale Dienste, öffentliche Verwaltung und Lebensmittelproduktion in Deutschland sind betroffen, abhängig von Größe und Jahresumsatz. Neu ist die persönliche Verantwortung des Managements: Geschäftsführende sowie leitende Managerinnen und Manager müssen sicherstellen, dass Risikomanagement-Maßnahmen umgesetzt und überwacht werden. Sie sind verpflichtet, entsprechende Schulungen zu absolvieren – bei Verstößen gegen diese Verpflichtungen haften sie persönlich. Doch nicht nur die gesetzlichen Vorgaben sollten zum Handeln motivieren. „Es ist wichtig, Mitarbeitenden Sicherheit zu vermitteln, damit sie im Ernstfall gut vorbereitet sind“, betont Diana Kühn, Account Managerin bei der TÜV NORD Akademie.

Um Manager und Geschäftsführende bei ihren Pflichten zu unterstützen, bietet die TÜV NORD Akademie drei Schulungen mit unterschiedlichen Schwerpunkten an. Weiterer Bestandteil des umfassenden Schulungsangebots für Cyber- und Informationssicherheit ist der vier-tägige Zertifikatslehrgang „NIS-2-Experte (TÜV)“ für Sicherheits- und IT-Verantwortliche. „Wenn die Teilnehmenden aus dem Seminar rausgehen, verstehen sie die gesetzlichen Anforderungen und können sie auf ihr Unternehmen anwenden“, so Braunschweig.

Seit September 2024 wurde der Lehrgang bereits elf Mal erfolgreich durchgeführt, für 2026 sind mindestens 18 weitere Schulungstermine geplant. „Die steigende Nachfrage bestätigt unsere frühe strategische Ausrichtung und unsere Expertise in der praxisnahen Vermittlung“, resümiert Kühn.





Melanie Braunschweig, Produktmanagerin bei der TÜV NORD Akademie, und **Diana Kühn**, Account Managerin bei der TÜV NORD Akademie

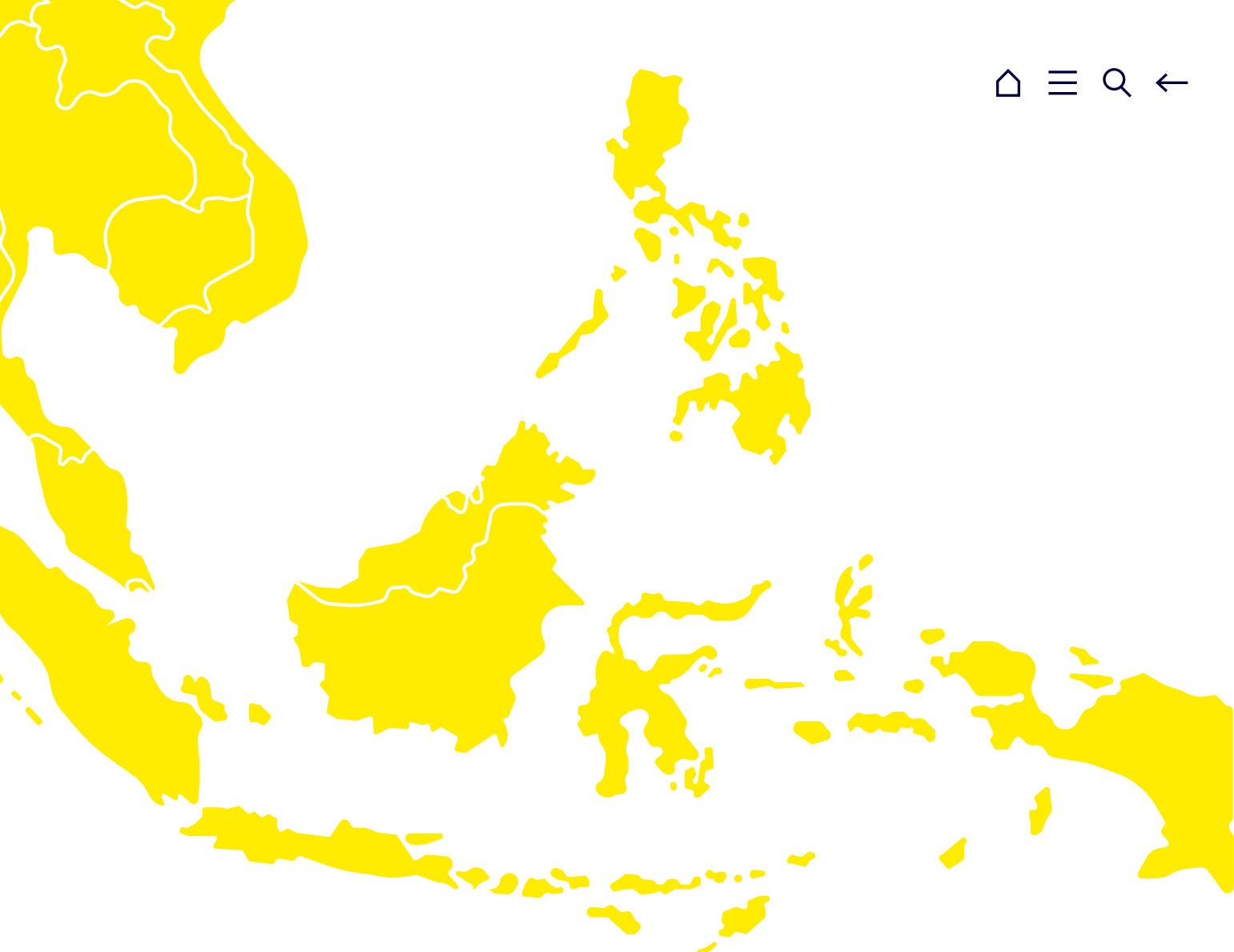


Digitale Transformation startet in Indonesien



Der Digital Hub SEA ist der Ausgangspunkt für eine Cloud-first-Plattform, die internationale Einheiten vernetzt und eine neue digitale Arbeitsweise ermöglicht. Südostasien dient nach den Worten von Dr. Jörg Aign, Geschäftsführer TÜV NORD International, als Pilotregion, um in einem dynamischen Umfeld eine belastbare Blaupause für die globale Transformation zu entwickeln, mit Fokus auf KI-gestützte Produktivität und Sicherheit.

Dr. Jörg Aign, Geschäftsführer
TÜV NORD International



Was verbirgt sich hinter dem Digital Hub SEA?

Der Digital Hub SEA ist der Startpunkt für unsere Cloud-first-Plattform, die künftig alle internationalen Einheiten verbindet und die Grundlage für eine neue digitale Arbeitsweise schafft. Wir gießen sozusagen ein sicheres Fundament, auf dem wir ein ganzes digitales Haus errichten. Wir entwickeln die Plattform in einem geschützten Umfeld, optimieren sie und rollen sie dann global aus. So schaffen wir die Basis für KI-gestützte Produktivität, weltweit standardisierte Prozesse und neue digitale Services.

Warum wurde gerade Südostasien, speziell Indonesien, als Pilotregion ausgewählt?

Südostasien gehört zu den dynamischsten Wirtschaftsregionen der Welt: Hier leben über 680 Millionen Menschen, die digitale Wirtschaft erreicht aktuell einen Bruttowarenwert von mehr als 300 Milliarden US-Dollar und Wachstumsraten von rund 4,5 Prozent. In Indonesien wollen wir die neue Plattform sicher entwickeln und erproben. Hier finden wir ideale Voraussetzungen, um schnell Erfahrungen zu sammeln und eine belastbare Blaupause für die globale Transformation zu entwickeln. Wir wollen die Plattform für den Einsatz von Copilot von Microsoft möglichst bald global ausrollen. Indem wir unsere Mitarbeitenden von Routinetätigkeiten entlasten und sie bei vielschichtigen Auswertungen und Analysen unterstützen, steigern wir ihre persönliche Produktivität.

Ziel ist es also, die Produktivität zu steigern, Prozesse zu vereinheitlichen und zu automatisieren sowie Daten zusammenzuführen?

Das ist richtig, aber auch nur der Anfang. Wir reden über eine Transformation in mehreren Dimensionen. Neben der schon erwähnten Steigerung der Produktivität automatisieren wir komplexe Geschäftsprozesse mithilfe von Power-Apps, Copilot Studio und Foundry IQ. Das sind Werkzeuge, die uns dabei unterstützen, digitale Lösungen zu entwickeln und Geschäftsprozesse zu optimieren. Wir wollen schnell und zuverlässig Daten von mehreren Speicherorten zusammenführen, um sie leicht nutzbar zu machen. Wir wollen schnell Geschäftsprozesse digitalisieren, ohne IT-Spezialistinnen und -Spezialisten einzubinden. Und wir wollen neue digitale Produkte entwickeln. Damit geht es nicht nur um Effizienz, sondern um die Neuausrichtung unserer Arbeitsweise und die Entwicklung neuer Chancen für den Konzern.

Wie geht das konkret?

E-Mails zusammenfassen, Texte entwerfen, Daten analysieren – das sind Aufgaben, die Microsoft Copilot gut erledigen kann. Später wollen wir mithilfe KI-gestützter Software, sogenannter Agenten, spezifische Aufgaben automatisiert erarbeiten lassen. Sie werden uns bei komplexen Aufgaben unterstützen. Aber immer unter menschlicher Kontrolle. KI ist eine helfende „Hand“, die uns entlastet: Copilot kann während eines Meetings automatisch mehrsprachige Notizen erstellen und die wichtigsten Entscheidungen live zusammenfassen. So sind alle Teilnehmenden sofort auf dem gleichen Stand – ohne Nacharbeit und Sprachbarrieren. Das ist ein Beispiel für das, was wir in Südostasien erproben und dann so schnell wie möglich für alle im Konzern verfügbar machen werden.

Können Sie der KI insbesondere bei der Lösung komplexer Aufgaben vertrauen?

Gerade bei komplexen Aufgaben zeigt KI perspektivisch ihre Stärke. Das erforderliche Vertrauen entsteht dabei durch Transparenz und Erfahrung. Wir setzen auf das Prinzip „Human in the Loop“: KI ist, wie gesagt, die helfende Hand. Moderne Datenplattformen wie Microsoft Fabric IQ gehen weit über das reine Sammeln und Speichern von Informationen hinaus. Sie verknüpfen Daten aus vielen Quellen, bereiten sie intelligent auf und machen sie für Analysen, KI-Modelle und Automatisierung nutzbar. Es entsteht eine echte „Intelligence Platform“, die Daten in Wissen, Prognosen und konkrete Empfehlungen verwandelt. Foundry IQ setzt dann als Wissens- und Kontextschicht für KI-Agenten darauf auf und ermöglicht die Entwicklung, das Training und den sicheren Betrieb von KI-Lösungen, die direkt in Geschäftsprozesse integriert werden können, etwa für vorausschauende Analysen, automatisierte Workflows oder intelligente Entscheidungsunterstützung in Bereichen wie Finanzen, dem operativen Betrieb oder Strategie. Dadurch stehen Informationen jederzeit aktuell, sicher und skalierbar zur Verfügung. KI kann komplexe Zusammenhänge erkennen und konkrete Empfehlungen geben, die allerdings immer von Menschen bewertet werden. Alle Prozesse bleiben transparent.



Das Team in Indonesien arbeitet fokussiert am zukunftsweisenden Digitalisierungsprojekt.



Aufbau einer Infrastruktur für Datenintegration, also das Zusammenführen von Daten aus unterschiedlichen Quellen.

Steigerung der Geschäftsproduktivität durch die Automatisierung komplexer Geschäftsprozesse mithilfe von KI und der Nutzung von Power-Apps.



Steigerung persönlicher Produktivität durch den Einsatz von KI bei Routine-tätigkeiten.



KI läuft nicht unbedingt auf dem Notebook, sondern eher serverbasiert ...

Richtig. Wir setzen auf eine hybride IT-Architektur, die Cloud und lokale Infrastruktur kombiniert. Die Intelligenz liegt in der Cloud, wo wir Skalierung, Sicherheit und Performance garantieren können. Sensible Daten und vertrauliche Arbeiten werden gezielt geschützt und, wo notwendig, in speziell abgesicherten Cloud-Umgebungen oder lokal verarbeitet.

Wollen Sie das Wissen, das Sie in Südostasien gewinnen, auch in anderen Regionen nutzen?

Das ist der Kern des Projekts: lernen, skalieren, wiederverwenden. Was wir in Südostasien entwickeln, wird die Blaupause für alle anderen Regionen. Und wir gehen noch weiter: Gute Lösungen, die irgendwo auf der Welt entstehen, werden global geteilt. Auf diese Weise vermeiden wir doppelte Aufwände, erhöhen die Effizienz und beschleunigen die Einführung neuer Technologien weltweit.



Engagiert und motiviert geht das Team in Indonesien nach dem Kick-off für die Power-Plattform die anstehenden Aufgaben an.



Der Digital Hub SEA ist der Startpunkt für unsere Cloud-first-Plattform, die künftig alle internationalen Einheiten verbindet und die Grundlage für eine neue digitale Arbeitsweise schafft.

Gute Lösungen, die irgendwo auf der Welt entstehen, werden global geteilt. So vermeiden wir doppelte Aufwände, erhöhen Effizienz und beschleunigen die Einführung neuer Technologien weltweit.



„Unser Digital Hub SEA macht uns schneller, effizienter und sicherer. Er eröffnet uns auch neue Geschäftsfelder.“

Dr. Jörg Aign, Geschäftsführer TÜV NORD International

Das hätte dann Auswirkungen auf den gesamten Konzern ...

Genau das ist die Vision. Südostasien ist der Startpunkt für unsere grundlegende globale IT-Transformation. Am Ende arbeiten wir alle auf einer sicheren, Cloud-first- und KI-fähigen Plattform. Die TÜV NORD GROUP wird dadurch zu einem agilen, datengetriebenen und vertrauenswürdigen Partner – mit Sicherheit als unverrückbarer Grundlage.

Digitale Sicherheit ist heute ein wichtiges Thema: Wird sie auch bei Ihnen mitgedacht?

Sicherheit ist das Fundament unserer Plattform. Wir setzen auf eine moderne Sicherheitsarchitektur mit „Zero Trust“ als Grundprinzip. Das bedeutet: Weder Nutzende noch Gerät oder Anwendung erhalten automatisch Vertrauen, egal ob innerhalb oder außerhalb des Unternehmensnetzwerks. Jeder Zugriff wird konsequent überprüft, jede Berechtigung ist auf das absolut Notwendige beschränkt und zeitlich begrenzt. So wird verhindert, dass sich Angreifer im System ausbreiten können, selbst wenn sie einen Zugangspunkt kompromittieren.

Kann eine solche Plattform zur Entwicklung des Unternehmens beitragen?

Ja, und zwar massiv. Sie macht uns schneller, effizienter und sicherer. Aber vor allem eröffnet sie neue Geschäftsfelder: datenbasierte Services, digitale Prüfmodelle, KI-gestützte Analysen, um einige zu nennen. Sie verwandelt uns in ein datengetriebenes Unternehmen, integriert KI in unsere Prozesse und ermöglicht es uns, neue Geschäftsmodelle zu entwickeln. Die Plattform ist damit das Fundament für nachhaltigen Erfolg und die Zukunft unseres Geschäfts. Wir lernen, probieren aus, entdecken neue Wege der Zusammenarbeit und entwickeln uns Schritt für Schritt weiter. Entscheidend ist, dass wir diesen Weg als Team gehen. KI unterstützt uns, erweitert unsere Möglichkeiten und gibt uns Freiraum für das, worin der Mensch mit seinem Wissen unschlagbar ist und bleibt. Gemeinsam gestalten wir so die Zukunft unseres Unternehmens, und genau das macht unseren Erfolg aus.

Impressum

Herausgeber

TÜV NORD AG
Am TÜV 1
30519 Hannover
tuev-nord-group.com
info@tuev-nord-group.com

Redaktion

3st kommunikation, Mainz

Konzeption und Gestaltung

3st kommunikation, Mainz

Fotografie

Adobe Stock [S. 12, 16]
Moritz Frankenberg [S. 20 unten]
Felix Matthies [S. 16 oben links, 23 – 24]
Christian Nielinger [S. 12 oben]
Samsung Electronics [S. 19]
Jeff Schad [S. 8 – 9]
Henning Scheffen [S. 4 – 5]
Frauke Schumann [S. 11, 15, 19 oben links, 23 oben]
Eric Shambroom [S. 6 – 7]
Dieter Sieg [S. 20]
TÜV NORD GROUP [S. 19 oben Mitte + oben rechts, 27 – 28]
Peter Venus, Capital Headshots Berlin [S. 16 oben rechts]



charta der vielfalt

UNTERZEICHNET

TÜV NORD AG
Am TÜV 1
30519 Hannover
Telefon +49 511 998-0
tuev-nord-group.com
info@tuev-nord-group.com
