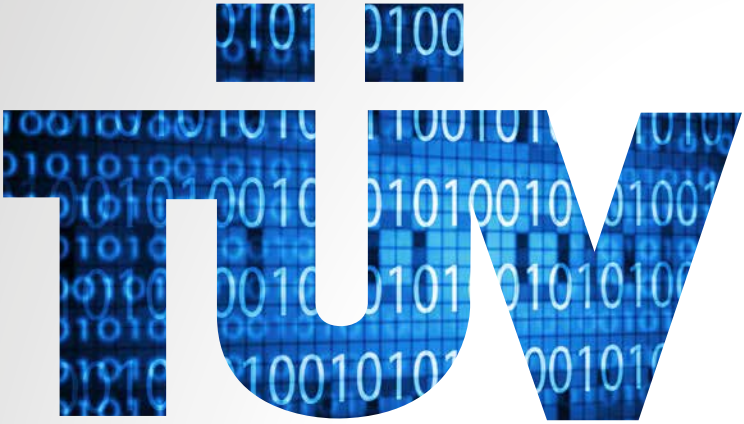
# Verband der TÜV e. V.

## Vertrauen und Akzeptanz in der digitalen Welt




TÜV®

# VORWORT

Die Digitalisierung steht in einer Reihe zahlreicher wirtschaftlicher Megatrends für einen enormen technologischen Wandel, der neue Märkte hervorgebracht und brancheninterne Spielregeln radikal umgewälzt hat. Fast alle Hersteller statten heute ihre Produkte und Industrieanlagen mit Sensoren und Connectivity aus. Das Internet der Dinge dringt so in alle Lebens- und Wirtschaftsbereiche vor. Hochinnovative Produkte wie beispielsweise medizinische Geräte oder vernetzte Fahrzeuge verfügen über eigene IP-Adressen und eine integrierte Software, über die die Funktion und Wirkung des Produkts oder einzelner Komponenten webbasiert manipuliert werden können. Dies trifft gerade auch auf kritische Infrastrukturen, also neuralgische Systeme wie die Strom- und Wasserversorgung, zu. Alle neuen, digital vernetzten Systeme und Produkte stellen Herausforderungen sowohl an die Cybersecurity gegen Hacker-Angriffe und Virenbefall als auch an den Datenschutz dar. Cybersecurity, Datenschutz und Vertrauenswürdigkeit digitaler Systeme sind wesentliche Voraussetzungen für Innovation und wirtschaftliches Wachstum.

# INHALT

# KERNFORDERUNGEN ZU CYBERSECURITY UND DATENSCHUTZ

1. Cybersecurity von digitalen Dienstleistungen und IT-vernetzten Produktionsanlagen sowie kritischen Infrastrukturen stärken! Vertrauen in die digitale Welt durch Zertifikate unabhängiger Dritter fördern!

2. *Security by Design*-Standards und Interoperabilität vorantreiben! Sie sind die Voraussetzung für den Erfolg der Digitalisierung. Hierfür müssen einheitliche europäische Standards für die digitale Vernetzung übergreifend definiert werden.

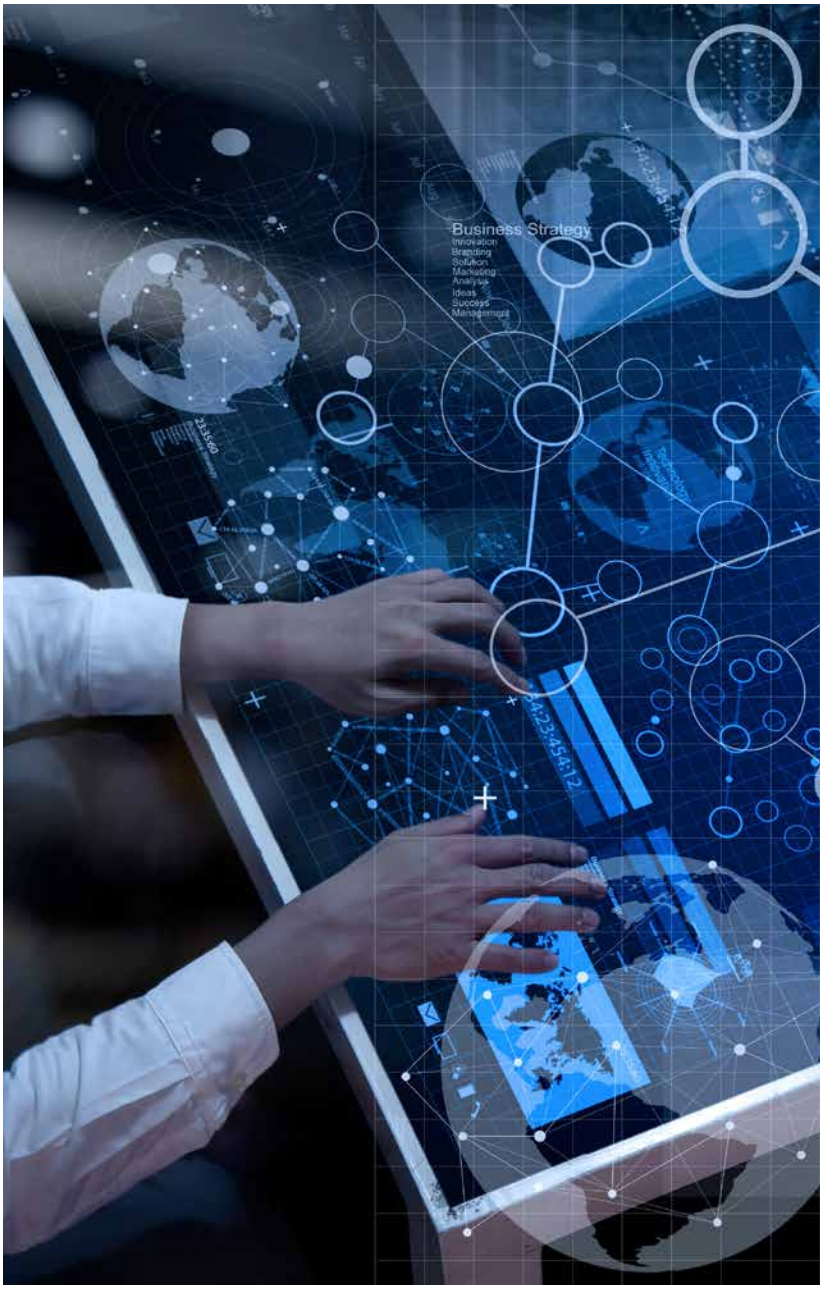
3. Die Prüfung von IoT-Produkten muss stets erweiterte Funktionalitäten wie Kommunikationsfähigkeit und Interoperabilität sowie die Aspekte *Safety* und *Security* umfassen.

4. Die Akzeptanz und Vertrauenswürdigkeit von Cloud-Lösungen durch international anerkannte Sicherheitsstandards und Datenschutzregelungen verbessern! Sie sind die Grundlage für Zertifizierungen und ein allgemein anerkanntes neutrales Prüfsiegel, das Seriosität, Qualität und Sicherheit einer Cloud-Dienstleistung vermitteln kann.

5. Schaffung eines unabhängigen und fachkompetenten Zulassungs- und Zertifizierungssystems für vertrauenswürdige und sichere Software-Lösungen vernetzter Geräte. Voraussetzung ist hierfür der diskriminierungsfreie Zugang zu Steuerungs- und Softwaredaten zu Prüfzwecken.

6. Die Verfügungsgewalt des Nutzers über seine personenbezogenen Daten muss gewährleistet bleiben! Diese Anforderungen an den Datenschutz sollten vor der Vermarktung digital vernetzter Produkte und Webservice-Anwendungen durch ein unabhängiges und qualifiziertes Audit und Zertifikat nachgewiesen werden.

7. Digitale Kompetenz der Gesellschaft durch gezielte Aus- und Weiterbildungsangebote bereits in der Schulausbildung stärken! Zur Steigerung der Beurteilungskompetenz bedarf es umfangreicher Sensibilisierung zu den Themen Cybersicherheit und Vertrauenswürdigkeit aller Mitarbeiter in Unternehmen und Behörden.


Business Strategy
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

# 1. INDUSTRIE 4.0 UND CYBERSECURITY ALS STRATEGISCHE FAKTOREN - VERTRAUEN IN DIE DIGITALE WELT DURCH UNABHÄNGIGE AUDITS UND ZERTIFIZIERUNGEN SCHAFFEN

Nach Mechanisierung, Elektrifizierung und Digitalisierung der Industrie leitet der breite Einsatz leistungsfähiger Datennetze in der Industrie und Wirtschaft eine vierte industrielle Revolution ein. Durch die Echtzeitkommunikation von Maschinen, Lagersystemen und Betriebsmitteln mit digitalen Systemen werden völlig neue Arten von Produktionsprozessen ermöglicht. Maschinen, Produkte, Fahrzeuge und Programme können durch den permanenten Austausch großer Datenmengen miteinander kommunizieren und sind somit in der Lage, effizienter miteinander zu arbeiten, sich zu optimieren und Fehler selbst zu erkennen. Die Anwendung smarter Dienste kann der Wirtschaft einen gewaltigen Wachstumsschub bringen. Wertschöpfungs- und Geschäftsmodelle der industriellen Produktion können völlig neu gestaltet werden, was wiederum erhebliche Auswirkungen auf den traditionellen Arbeitsmarkt hat. Der VdTÜV ist davon überzeugt, dass Europa die neusten Entwicklungen der digitalen Welt in der Produktion intelligent einsetzen muss, um eine höhere Effizienz und Wettbewerbsfähigkeit in der Industrie zu erreichen. Hierzu sind einheitliche Rahmenbedingungen für branchen- und grenzüberschreitende Technologiepartnerschaften erforderlich.

Gleichzeitig birgt eine wachsende Abhängigkeit von intelligenten, digital vernetzten Gegenständen auch die Notwendigkeit der Absicherung informationstechnischer Systeme vor Cyberattacken und Datenmanipulationen. Der VdTÜV setzt sich daher für ein neues umfassendes Sicherheitsverständnis ein. Neue Technik muss vorausschauend neben der funktionalen Sicherheit *(Safety)* auf Kriterien wie *Security by design/default* und auch *Privacy by design/default* in der Entwicklungsphase und in der fertigen Umgebung über die gesamte Wert-

schöpfungskette und gegebenenfalls im Betrieb unabhängig bewertet und geprüft werden. Unabhängige Zertifizierungen und Prüfungen durch akkreditierte neutrale Dritte liefern den verlässlichen Nachweis, dass diese Kriterien eingehalten werden. Sie sorgen für Transparenz und das notwendige Vertrauen in Produkte, Prozesse und neue Technologien.

## Exkurs: Trust4safety

Die Notwendigkeit von *Safety*-Maßnahmen (Unversehrtheit des Menschen, Betriebssicherheit) ist unbestritten. Da aber alle Energie- und Datennetze digital gesteuert werden, der Vernetzungsgrad und die Datenflut weiter ansteigen, wächst die Verwundbarkeit der Anlagen durch Cyber-Attacken. Die Betriebssicherheit (*Safety* nach ISO 61508) in der Industrie muss in das Internet der Dinge (IoT) mit Anforderungen an die Interoperabilität, den Transaktionsschutz, erweiterbare Funktionen etc. eingebunden und konsequent in Verbindung mit der Cybersecurity verstanden und gemanagt werden *(trust4safety)*. Die entsprechende Kompetenz und Expertise muss aus allen Bereichen zusammengebracht werden. Die Einbindung der *Safety*-Komponente in das IoT und die Cybersecurity stellen somit für die Industrie einen strategischen Faktor dar. Ihre Berücksichtigung als integraler Bestandteil ab der Produktentwicklung über dessen gesamte Lebensdauer wird über den Erfolg und die Akzeptanz der digitalen Vernetzung in Industrie und Gesellschaft maßgeblich entscheiden.

*Security by Design*-Standards und Interoperabilität müssen stärker gefördert und als einheitliche europäische Standards für die digitale Vernetzung übergreifend definiert werden. Hierzu muss sich Deutschland noch stärker an entsprechenden europäischen und internationalen Normungs- und Standardisierungsgremien beteiligen.


## Kritische Infrastrukturen sichern – Präventions- und Reaktionspflichten ausweiten

Alle Unternehmen stehen vor der Herausforderung eine ganzheitliche Informationssicherheitsstruktur aufzubauen. Die Einführung entsprechender IT-Sicherheitsmaßnahmen trägt wesentlich zur Prävention bei und kann im Ernstfall den Zeitraum zwischen dem Erkennen einer Cyberattacke und der Behebung des Problems auf ein Minimum reduzieren.

Viele Unternehmen können heute offenbar ihre eigenen Sicherheitsrisiken ohne eine entsprechende Expertise nicht aufdecken. Ein Drittel der Sicherheitslücken in den Unternehmen wird nicht von internen IT-Sicherheitsteams entdeckt, sondern von Experten außerhalb des Unternehmens. Die Angriffsflächen sind zu komplex und mannigfaltig, als dass sie dauerhaft ausgeschlossen werden könnten. Dennoch stellen Unternehmensverbände zunehmend herstellerunabhängige Prüfungen und Zertifizierungen neutraler Instanzen

in Frage. Der VdTÜV ist dagegen der Überzeugung, dass Unternehmen die Expertise unabhängiger, qualifizierter Stellen für Sicherheitsaudits, Zertifizierungen und regelmäßige Überprüfungen der IT-Sicherheitsarchitektur nutzen müssen, um die Sicherheit und Akzeptanz in die digitale Wirtschaft zu stärken. Unabhängige Audits und deren kontinuierliche Überprüfung bedeuten einen besseren präventiven Schutz gegen IT-Angriffe als Eigenüberwachungen der Wirtschaft und vermitteln zudem glaubhaft, dass die IT-Sicherheitsarchitektur ein adäquates Schutzniveau erfüllt.

Nach Einschätzung des VdTÜV zeigt das IT-Sicherheitsgesetz in die richtige Richtung, allerdings sieht das Gesetz unter gewissen Auflagen Selbstzertifizierungen von Unternehmen vor, die der VdTÜV für nicht zielführend hält. Zudem sind die derzeit in den Verordnungen des IT-Sicherheitsgesetzes festgelegten Grenz- und Schwellenwerte für kritische Infrastrukturen (KRITIS) zu hoch angesetzt. Da auch der Ausfall kleinerer Wasserwerke oder Energieversorger bereits zu erheblichen Versorgungsengpässen führen kann, fordert der VdTÜV dringend eine Anpassung der verordnungsrechtlichen Bestimmungen und die Ausweitung des Anwendungsbereichs des IT-Sicherheitsgesetzes auf den Bereich der Zulieferer von KRITIS-Unternehmen. Denn Unternehmen werden zukünftig ohnehin von ihren Lieferanten weitere Sicherheitsnachweise bis hin zu einem ISO 27001-Zertifikat verlangen.

## Cloud-Dienste sicher machen

Viele Unternehmen lehnen bislang wegen Sicherheitsbedenken das Verlagern von Daten in eine Cloud ab, obwohl es im Hinblick auf eine Effizienzsteigerung - besonders für den Mittelstand - viele Vorteile bringen kann. Aus diesem Grund sind international anerkannte Sicherheitsstandards sowie unabhängige, vertrauenswürdige, aber vor allem professionelle Zertifizierungen notwendig, um eine verlässliche Aussage über die Qualität und Vertrauenswürdigkeit eines Cloud-Dienstes, seines Anbieters und aller nachgelagerten Prozesse wie

Sicherheit, Infrastruktur, Verfügbarkeit usw. zu gewährleisten. Dabei sollte der Cloud-Dienst hinsichtlich der Kriterien Prozess- und Aufbauorganisation, Datensicherheit, Compliance/Datenschutz und der Nutzerfreundlichkeit der Cloud von unabhängiger Seite geprüft werden. Die Speicherung von Daten muss verschlüsselt erfolgen, um eine nachträgliche Personalisierung von Daten in einer gemeinschaftlich genutzten Cloud zu verhindern. Hierfür sind europaweit einheitliche Regelungen für die Standardisierung und Zertifizierung des Datenschutzes in der Cloud unerlässlich. Sie sind auch die Grundlage für ein allgemein anerkanntes neutrales Prüfsiegel, das Seriosität, Qualität und Sicherheit einer Cloud-Dienstleistung vermitteln kann.

## Zertifizierung und Zulassung von IT-Produkten stärken

Ziel ist es, den Zugang zu sicheren und vertrauenswürdigen IT-Produkten für Wirtschaft, Gesellschaft und Staat zu ermöglichen, damit diese die Vorteile der Digitalisierung nutzen können. Bei der Vermarktung von IT-Produkten spielen Marketing- und Preisgesichtspunkte eine deutlich wichtigere Rolle als die Sicherheit digital vernetzter Produkte. Oftmals erweckt auch die Beschreibung des Produkts falsche Erwartungen über die Einsatzmöglichkeit beim Nutzer. Gleichzeitig wächst die Zahl der Produkte mit gravierenden Software-Schwachstellen. Hierbei handelt es sich um alle Produkte, Systeme und Anwendungen, die softwarebasiert operieren, von kritischen Infrastrukturen bis hin zu Produkten der privaten Nutzung (Elektro- und Haushaltsgeräte, Werkzeuge, Spielzeuge etc.). Im Rahmen der Zertifizierung muss nachgewiesen werden, dass das jeweilige Produkt bestimmte funktionale und grundlegende Sicherheitseigenschaften erfüllt, die in entsprechenden Schutzprofilen, Sicherheitsvorgaben oder Technischen Richtlinien spezifiziert sind. Zukünftig muss es auch für Softwareanbieter zu definierende Haftungsauflagen geben, die sicherstellen, dass sie auch dann noch ihrer Sorgfaltspflicht nachkommen, wenn sie die Software bereits verkauft haben.

Das IT-Sicherheitsgesetz und die europäische Cybersicherheits-Richtlinie müssen daher so fortentwickelt werden, dass ein unabhängiges und fachlich kompetentes Zulassungs- und Zertifizierungssystem für eine vertrauenswürdige und sichere Software vernetzter Geräte ausreichende Schutzstandards setzt und gleichzeitig Innovationszyklen sowie zeitnahen Markteintritt ermöglicht. Dazu gehören entsprechende Interoperabilitäts- und Funktionalitätstests bei der Zulassung und Zertifizierung digital vernetzbarer Produkte und Geräte, um eventuelle Manipulationen oder Fehlfunktionen zu erkennen. Voraussetzung ist hierfür der diskriminierungsfreie Zugang zu Steuerungs- und Softwaredaten zu Prüfzwecken im Rahmen der Produktzulassung.


## Regulativer Nachbesserungsbedarf in Europa bei IoT-Produkten

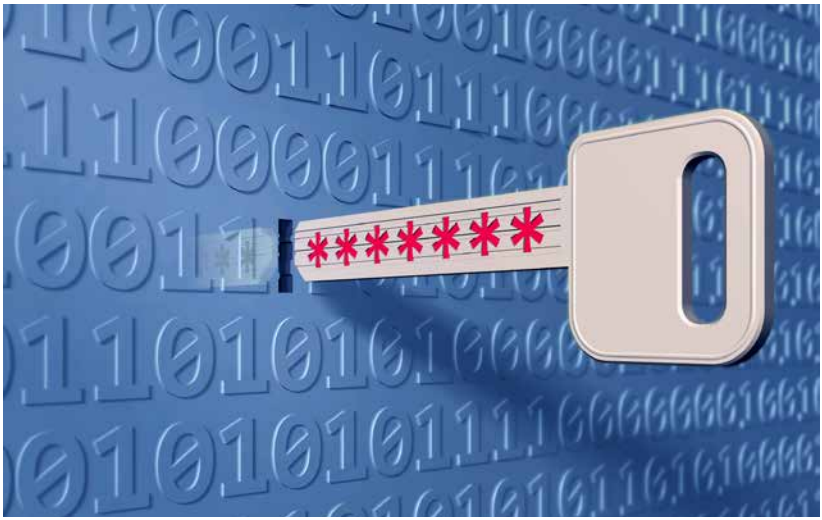
Der europäische Gesetzgeber ist verpflichtet, ein hohes Schutzniveau für die Verbraucher sicherzustellen. Demzufolge muss der europäische Regulierungsrahmen gewährleisten, dass alle Menschen Vertrauen in die Sicherheit von

digital vernetzten (IoT) Produkten setzen können, damit diese Innovationen die notwendige Akzeptanz erfahren.

Wenn IoT-Produkte in Verkehr gebracht werden, muss dafür Sorge getragen werden, dass sie voll funktionsfähig, interoperabel und sicher sind. Bei allen IoT-Produkten sollte geprüft werden, ob durch deren Anbindung an das Internet zusätzliche Bedrohungen auftreten können, die die ordnungsgemäßen, bisher geprüften Leistungsmerkmale in Frage stellen. Mit einer IoT-Richtlinie, die den jeweiligen Stand der technischen Entwicklung abbildet, wären gesonderte und erweiterte Prüfprozesse für vernetzte Produkte verpflichtend. Analog zu den Prüfverfahren für nicht digital vernetzte Produkte sollte auf die Kompetenz qualifizierter und unabhängiger Stellen zurückgegriffen werden.

## 2. ZUGANG UND NUTZUNG VON DATEN SICHER UND VERTRAUENSWÜRDIG ERMÖGLICHEN

Die digital vernetzte Wirtschaft steht im Spannungsfeld zwischen der umfassenden Nutzung, Anwendung, Funktionalität der Produkte auf der einen Seite und den gesetzlichen Datenschutzbestimmungen sowie der IT Sicherheit auf der anderen Seite. Oberste Gebote einer modernen Datenpolitik müssen der Schutz des Rechts auf Privatsphäre des Verbrauchers, des Grundrechts auf informationelle Selbstbestimmung bzw. die Wahlfreiheit des Verbrauches im Umgang mit seinen Daten sein. Dazu ist Transparenz notwendig: Die Verbraucherinnen und Verbraucher sind angemessen zu informieren, so dass sie in der Lage sind, den Datenfluss nachzuvollziehen bzw. eine bewusste Entscheidung darüber treffen zu können, welche Daten wann, zu welchem Zweck, zu welchen Bedingungen und für welche private oder staatliche Stelle zur Verarbeitung zugänglich gemacht werden sollen.



In Analogie zum Eigentumsrecht soll jeder die Verfügungsgewalt über seine personenbezogenen Daten haben. Für die Sicherheit können passende und moderne Signaturtechniken sowie zusätzliche Schutzmechanismen, wie zum Beispiel besondere Verschlüsselungsmethoden, Identifizierung der Zugriffe oder Informationsflusskontrollen sorgen. Grundsätzlich gilt es zu vermeiden, dass persönliche Daten auf Servern außerhalb der physischen Zugriffsmöglichkeit und der Rechtsprechung des Wirkungsbereichs der europäischen Datengrundschutzverordnung gespeichert werden, wenn dort kein mit der EU vergleichbares Datenschutzniveau besteht. So muss die Datenverarbeitung beispielsweise in einem Fahrzeug bereits bei Entwicklung und Auslieferung an den Kunden die Anforderungen von Privacy by design und Privacy by default berücksichtigen. Personenbezogene Daten sollten prinzipiell im Auto selbst verbleiben. Wenn sie transferiert oder weiterverarbeitet werden sollen, dann nur anonymisiert oder pseudonymisiert an den externen Server. Diese Anforderungen an den Datenschutz sollten vor der Vermarktung digital vernetzter Produkte und Webservice-Anwendungen durch ein unabhängiges und qualifiziertes Audit und Zertifikat nachgewiesen werden.

Zur Schaffung eines einheitlichen und interoperablen Markts in der EU sollte eine europäische Gesetzesinitiative dafür sorgen, dass sich Datenströme über Grenzen und Sektoren hinweg bewegen können und Daten bestmöglich zwischen Verbrauchern, Herstellern und Serviceanbietern verfügbar gemacht und weiterverwendet werden. Grundlage hierfür sollte die ab Mai 2018 verbindlich geltende EU-Datenschutzgrundverordnung sein.


## 3. SENSIBILITÄT UND VERSTÄNDNIS FÜR CYBERSICHERHEIT FÖRDERN

Ohne ein IT-Grundverständnis und einen verantwortungsvollen Umgang in der Gesellschaft, Wirtschaft und Politik werden alle gesetzlichen Rahmenbedingungen nicht ausreichen, um die IT-Sicherheitslage zu verbessern. Denn auch mangelndes Sicherheitsbewusstsein der Nutzer macht ein IT-System angreifbar. Rein technische Maßnahmen allein genügen nicht, Cybersecurity-Bedrohungen abzuwehren. Erst die Sensibilisierung der Nutzer für

Sicherheitsmaßnahmen und grundsätzliches Wissen über Cybersecurity schaffen nachhaltigen Informationsschutz auf hohem Niveau und ermöglichen ein sicheres und selbstbestimmtes Handeln des Einzelnen in einer digitalisierten Umgebung. Berufsbegleitende, lebenslange Schulungen der Angestellten spielen dabei eine immer größere Rolle. Dies bleibt eine gesellschafts- und bildungspolitische Herausforderung. Getreu ihrem Gründungsmotto leisten die TÜV-Unternehmen seit langem mit entsprechenden Schulungsangeboten „Hilfe zu Selbsthilfe und zum Selbstschutz“ für Arbeitgeber und -nehmer. Der digitale Wandel in Wirtschaft und Gesellschaft braucht sowohl klassische Berufsprofile als auch neue Expertenprofile mit Erfahrungen und Know-how in der Vernetzung von Industrieprozessen und IKT, die sich idealerweise ergänzen.

**Herausgeber**

Verband der TÜV e. V.

Friedrichstraße 136, 10117 Berlin

Tel.: +49 30 760095-400

Fax: +49 30 760095-401

E-Mail: berlin@vdtuev.de

www.vdtuev.de

www.twitter.com/vdtuev_news

Fotos

© iStock.com / MF3d; Prykhodov

© extradeda; andrey_l; solarseven; ESB Professional / Shutterstock.com