Verband der TÜV e. V.

Vertrauen und Akzeptanz in der digitalen Welt

TÜV®

VORWORT

Produktion und Dienstleistungen in unserer Wirtschaft basieren zunehmend auf digitaler Vernetzung. Daten- und Informationssicherheit sind ein wichtiger Standortfaktor für die deutsche Wirtschaft. Gleichzeitig werden die Wirtschaft, der Staat und die Bevölkerung mit einer wachsenden Anzahl skrupelloser Cyber-Kriminalität konfrontiert. Dazu zählen u. a. die Infiltration spezieller Netzwerke, das gezielte Ausspähen und die rasche Proliferation bzw. der Verkauf von sensiblen Daten und Informationen über potenzielle Schwachstellen in Unternehmen.

Zwischen 2013 und 2014 hat sich die Zahl der gemeldeten Cyberangriffe weltweit um 48 Prozent auf insgesamt 42,8 Millionen erhöht. Hinzu kommt eine enorme Dunkelziffer. Daher bleibt die andauernde, sichere Vernetzung nach dem Stand der Technik in Gesellschaft und Industrie eine vorrangige strategische Aufgabe. Es kommt aus unserer Sicht darauf an, Daten- und Informationssicherheit in Unternehmen, Organisationen und Institutionen der öffentlichen Hand als strategische und lohnenswerte Investition zu begreifen und systematisch zu konzipieren. Denn trotz steigender Cyberangriffe sank im gleichen Zeitraum 2013 und 2014 die Bereitschaft großer Konzerne, höhere finanzielle Ressourcen für ihre Security bereitzustellen. Zudem ist eine IT-Sicherheitsforschung erforderlich, die auf die neuen Herausforderungen der digitalen Vernetzung reagiert sowie die Entwicklung und Erforschung risikobasierter Schutzkonzepte fördert. Herkömmliche Ansätze der IT-Sicherheit aus Perspektive der Endgeräte sind heute nicht mehr ausreichend.

Vor diesem Kontext hält der VdTÜV die Investition in Security und den Aufbau einer ganzheitlichen, kompatiblen Informationssicherheitsstruktur zur Stärkung von Vertrauen und Akzeptanz in der digitalen Welt für grundlegend wichtig.

Dr. Klaus Brüggemann
Geschäftsführendes Präsidiumsmitglied VdTÜV

Markus Bartsch
Vorsitzender VdTÜV-AK Cyber Security

INHALT

1. **Top-Forderungen des VdTÜV**
2. **Politische Grundsätze**
3. **Cyber Security als strategischer Faktor**
4. **Industrie 4.0 als Innovationsmotor für Europas Wirtschaft**
5. **Standardisierung und Zertifizierung**
6. **Verbesserter Schutz kritischer Infrastrukturen**
7. **Meldepflicht via TÜV-Treuhänder**
8. **Cloud-Computing sicher machen**
9. **Sensibilität und Verständnis für Cyber-Sicherheit – Fachkräfte qualifizieren**

1. TOP FORDERUNGEN DES VDTÜV

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

2. Die Betriebssicherheit (Safety) in der Industrie konsequent mit dem Schutz der digitalen Information (Security) bei IKT-Anwendungen vernetzen! (Safety-and-Security-by-Design)

3. Rechtsvorschriften und Normen in Deutschland und der EU harmonisieren und an die vernetzte Industrie anpassen! Branchen- und grenzüberschreitende Technologiepartnerschaften sowie einen gemeinsamen europäischen Markt hierdurch ermöglichen!

4. Sicherheitsorganisation kritischer Infrastrukturen durch unabhängige, akkreditierte Prüforganisationen regelmäßig überprüfen!

5. IT-Sicherheitsvorfälle in pseudonymisierter Form an die nationalen Sicherheitsbehörden melden!

6. Die Akzeptanz und Vertrauenswürdigkeit von Cloud-Lösungen durch international anerkannte Sicherheitsstandards sowie unabhängige, kompetente Zertifizierungen verbessern!

7. Die digitale Kompetenz unserer Gesellschaft durch gezielte Aus- und Weiterbildungsangebote bereits ab den Schulen stärken!

2. POLITISCHE GRUNDSÄTZE

Die TÜV-Unternehmen sehen die Bundesregierung in der Verpflichtung, durch die Schaffung eines funktionstüchtigen regulativen Rahmens auf ein hohes Schutzniveau der IT-Sicherheit von digitalen Dienstleistungen, Produktionsanlagen und kritischen Infrastrukturen hinzuwirken. Für den Standort Deutschland ist sein hoch-innovativer Mittelstand dabei von zentraler Bedeutung. IT-Technologie „Made in Germany" ist aufgrund staatlicher Datenschutzvorgaben weltweit gefragt. Die Förderung nationaler, vertrauenswürdiger IT-Sicherheitstechnologien und Investitionen in Forschung und Entwicklung müssen jetzt finanziell abgesichert und voran gebracht werden. Unabhängige Zertifizierungsprozesse in Unternehmen vermitteln den Verbrauchern glaubhaft, dass neue und intelligente Technologien auch sicher und vertrauenswürdig sind, und so diese die nötige Akzeptanz finden werden.

Der VdTÜV unterstützt in diesem Kontext die vorgeschlagene EU-Richtlinie zur Netz- und Informationssicherheit und das deutsche IT-Sicherheitsgesetz. Beide Vorschläge müssen einen abgestimmten rechtlichen Rahmen für mehr Kooperation und freiwillige Initiativen in der Cybersicherheit setzen. Hierdurch wird EU-weit einheitlich das Schutzniveau der IT-Sicherheit von digitalen Dienstleistungen und Produktionsanlagen sowie kritischen Infrastrukturen gestärkt.

3. CYBER SECURITY ALS STRATEGISCHER FAKTOR

Cyber Security ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber Security entsteht durch die Summe und das Ineinandergreifen von geeigneten und angemessenen Maßnahmen. Dies betrifft die Datenerzeugung, -übertragung, -speicherung und –auwertung über physische und nichtphysische Schnittstellen sowie die Berücksichtigung des Faktors Mensch.

Während die Notwendigkeit von Safety-Maßnahmen (Unversehrtheit des Menschen, Betriebssicherheit) unbestritten ist, herrscht im Bereich der Security (Schutz der digitalen Informationen) noch Unsicherheit über den benötigten Schutzbedarf. Entweder wird die Informationssicherheit nicht systematisch gemanagt oder die technische Umgebung wird getrennt von der IT betrachtet. Da aber alle Energie- und Datennetze digital gesteuert werden, der Vernetzungsgrad und die Datenflut weiter ansteigen, wächst auch die Verwundbarkeit der Anlagen durch Cyber-Attacken. Die Betriebssicherheit (Safety) in der Industrie muss konsequent in Verbindung mit der Cyber Security bei IKT-Anwendungen verstanden und gemanagt werden (Safety and Security by Design). Die entsprechende Kompetenz und Expertise muss aus beiden Bereichen zusammengebracht werden. Cyber Security stellt 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.

4. INDUSTRIE 4.0 ALS INNOVATIONSMOTOR FÜR EUROPAS WIRTSCHAFT

Nach Mechanisierung, Elektrifizierung und Digitalisierung der Industrie leitet der Einzug des Internets der Dinge in der Fabrik eine vierte industrielle Revolution ein. Durch die Echtzeitkommunikation von Maschinen, Lagersystemen und Betriebsmitteln mit digitalen Systemen werden völlig neue Arten von Produktionsprozessen ermöglicht. Maschinen können durch den permanenten Austausch großer Datenmengen miteinander kommunizieren und sind somit in der Lage, sich selbstständig zu steuern, effizienter miteinander zu arbeiten und Fehler selbst zu erkennen. Nutzer werden informiert, wenn Produkte ersetzt, repariert oder zurückgerufen werden müssen, sie noch frisch sind oder ihr Haltbarkeitsdatum überschritten haben.

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. Wertschöpfungs- und Geschäftsmodelle der industriellen Produktion können völlig neu gestaltet werden. Hierzu sind einheitliche Rahmenbedingungen für branchen- und grenzüberschreitende Technologiepartnerschaften erforderlich.

Aus Sicht des VdTÜV müssen die Rechtsvorschriften und Normen in Deutschland und der EU so angelegt sein, dass neue Produkte und Technologien im europäischen Binnenmarkt rasch in Umlauf gebracht werden können. Bei Industrie 4.0 sind Standards und der Aufbau von Referenzarchitekturen für die vernetzte Technologie cyber-physikalischer Systeme (CPS) unabdingbar. Unabhängige Zertifizierungen durch akkreditierte neutrale Dritte liefern den verlässlichen Nachweis, dass diese Standards eingehalten werden. Sie sorgen für Transparenz und das notwendige Vertrauen in Produkte, Prozesse und neue Technologien.

5. STANDARDISIERUNG UND ZERTIFIZIERUNG

Die größte Herausforderung für die digital vernetzte Produktion, für die Verkehrsmittel der Zukunft, das Smart Grid wie auch das Gesundheitswesen wird die Standardisierung darstellen. Die notwendige Integration der neuen vernetzten Systeme über Domänen- und Hierarchiegrenzen hinweg wird sich nur auf Basis internationaler, konsensbasierter Normen und Standards realisieren. Diese schaffen eine sichere Grundlage für die technische Beschaffung, unterstützen die Kommunikation durch einheitliche Begriffe und Konzepte und werden die Interoperabilität, Praxistauglichkeit und Marktrelevanz sicherstellen.

Um die Risiken zu minimieren und Schwachstellen zu beseitigen, bevor sie ein Hacker ausnutzen kann, sollte Security künftig bereits ein wesentliches Leistungsmerkmal des Entwicklungsprozesses sein. Die internationalen und in 26 Industrienationen von den nationalen Sicherheitsbehörden offiziell anerkannten „Common Criteria - CC“ verfolgen exakt diesen Ansatz. Diese CC müssten aber für industrielle Komponenten und Systeme noch entsprechend angepasst werden.

Zukünftig wird es für die Unternehmen viel wichtiger, das Sicherheitsniveau von IT-Lösungen und -Prozessen kontinuierlich zu überprüfen und das Informationssicherheits-Management-System (ISMS) durch eine Zertifizierung, zum Beispiel nach der internationalen Norm ISO/IEC 27001, zu optimieren. Zu den Vorteilen eines professionellen Informationssicherheits-Management-Systems zählt insbesondere die wirksame Kontrolle von IT-Risiken durch ein systematisches Risiko-Management. Somit können Schwachstellen aufgedeckt, Risiken sowie potenzielle Schäden und Folgekosten minimiert werden.

6. VERBESSERTER SCHUTZ KRITISCHER INFRASTRUKTUREN

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen der Bereiche Energie, Verkehr, IKT, Banken, Versicherungen, Börsen, Gesundheit und Ernährung, bei denen ein besonders hohes übergeordnetes gesellschaftliches Sicherheitsinteresse besteht. Für die dort implementierten, hochsensiblen IT-Systeme ist eine regelmäßige Überprüfung der Sicherheitsorganisation durch unabhängige, akkreditierte Prüforganisationen gesetzlich festzulegen. Sowohl Unternehmen mit kritischen Infrastrukturen als auch sicherheitssensible staatliche Stellen sollten angesichts zunehmender Hackerangriffe und Wirtschaftsspionage permanent die Widerstandsfähigkeit (Resilienz) der eigenen Prozesse und der eingesetzten Informations- und Kommunikationstechnik gegen Cyberbedrohungen stärken. Schließlich wird auch von dem Betreiber eines Fahrgeschäfts auf dem Jahrmarkt zu Recht verlangt, mit TÜV-geprüftem Gerät zu arbeiten, die Gäste richtig zu instruieren und alle weiteren notwendigen Sicherheitsmaßnahmen zu treffen.

Bereits etablierte, internationale IT-Security Standards müssen fortentwickelt und sukzessive weltweit harmonisiert werden. Sie sind für ein verlässlich hohes IT-Sicherheitsniveau in Unternehmen im Zeitalter der Globalisierung unabdingbar. Der Gesetzgeber ist gemeinsam mit der Wirtschaft gefordert, eine genaue Definition kritischer Infrastrukturen zu erarbeiten, die verbindliche Mindestanforderungen an die IT-Sicherheit erfüllen sollen.

7. MELDEPFLICHT VIA TÜV-TREUHÄNDER

Der VdTÜV begrüßt die Pläne zur Einführung einer Meldepflicht „schwerwiegender Beeinträchtigungen“ von informationstechnischen Systemen, Komponenten oder Prozessen für Betreiber kritischer Infrastrukturen. IT-Sicherheitsvorfälle sollen jedoch in pseudonymisierter Form an die nationalen Sicherheitsbehörden gemeldet werden. Einerseits wird so das Risiko von Reputationsschäden für das meldende Unternehmen minimiert. Andererseits haben die Behörden hierdurch die Möglichkeit, ein uneingeschränktes Lagebild zu erstellen, um mögliche Gegenmaßnahmen zum Schutz anderer Unternehmen einzuleiten. Gleichzeitig kann ein neutraler Rückkanal von der Sicherheitsbehörde an das Unternehmen implementiert werden, um aktuelle Informationen über Angriffe von der Behörde zu erhalten.

Die TÜV bieten sich hier als unabhängige Treuhänder an, denn sie verfügen bereits heute schon über das in der Praxis erprobte Know-how, einen entsprechenden nachvollziehbaren und auditierbaren Übermittlungsprozess in pseudonymisierter Form zwischen einem betroffenen Unternehmen und einer Behörde einzurichten.

8. CLOUD-COMPUTING SICHER MACHEN

Viele Unternehmen lehnen bislang wegen Sicherheitsbedenken das Verlagern von Daten in eine Cloud ab, obwohl es im Hinblick auf eine Effizienzsteigerung gerade 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 unerlässlich.

9. SENSIBILITÄT UND VERSTÄNDNIS FÜR CYBER-SICHERHEIT – FACHKRÄFTE QUALIFIZIEREN

Auch mangelndes Sicherheitsbewusstsein der Nutzer macht ein IT-System angreifbar. Rein technische Maßnahmen allein genügen nicht, Bedrohungen der IT-Sicherheit abzuwehren. Erst die Sensibilität der Nutzer für Sicherheitsmaßnahmen und grundsätzliches Wissen über Cyber-Security schaffen nachhaltigen Informationsschutz auf hohem Niveau. Dies ist gleichzeitig eine gesellschafts- und bildungspolitische Herausforderung. Denn bislang fehlen noch entsprechende Cyber-Security-Spezialisten. Daher sind insofern staatliche Anreizsysteme zu etablieren und gezielte Bildungsmaßnahmen durch Fördermittel zu unterstützen. Zudem müssen die Aus- und Weiterbildungscurricula bereits ab der Schule angepasst werden, um die digitale Kompetenz zu stärken. Berufsbegleitende, lebenslange Schulungen der Angestellten spielen eine immer größere Rolle. Der digitale Wandel in Wirtschaft und Gesellschaft braucht neue Expertenprofile mit Erfahrungen und Know-how in der Vernetzung von Industrieprozessen und IKT. Der Mensch muss für die Herausforderung Cyber-Security nachhaltig gerüstet werden.

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: istockphoto.com (Titel, 09); fotolia.com (02, 05, 07, 08); shutterstock.com (10)