Verband der TÜV e.V.

TÜV®

Verfasser
Richard Goebelt

Datum
11.03.2015

VdTÜV Input zur Digitalen Agenda „Vertrauen und Akzeptanz in der digitalen Welt“

Standpunkt 1

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

Digitale Technologien bewirken eine Disruption von Wirtschaft und Gesellschaft. Im Mittelpunkt dieses Paradigmenwechsels muss das Thema Sicherheit sowie die Wettbewerbs- und Zukunftsfähigkeit Europas stehen.

Der Gesetzgeber steht in der Pflicht, einen funktionstüchtigen regulativen Rahmen für ein hohes Schutzniveau digitaler Dienstleistungen, Produktionsanlagen und kritischen Infrastrukturen zu schaffen.

Die Förderung europäischer IT-Sicherheitstechnologien und Investitionen in Forschung und Entwicklung müssen finanziell abgesichert und voran gebracht werden.

Unternehmen, Organisationen und Institutionen der öffentlichen Hand müssen Daten- und Informationssicherheit als strategische und lohnenswerte Investition begreifen und systematisch konzipieren.

Das bedeutet den Aufbau einer ganzheitlichen, kompatiblen Informationssicherheitsstruktur zur Stärkung von Vertrauen und Akzeptanz in der digitalen Welt. Es müssen Lösungen gefunden werden, die vor allem darauf abzielen, den Zeitraum zwischen dem Erkennen einer Cyberattacke und der Behebung des Problems auf ein Minimum zu reduzieren. Eine wirksame Bekämpfung komplexer gezielter Angriffe kann daher nicht nur die Sicherheitsarchitektur, sondern muss das komplette Unternehmen, seine Prozesse sowie dessen Mitarbeiter miteinbeziehen. Unabhängige Zertifizierungen durch qualifizierte Stellen vermitteln den Verbrauchern glaubhaft, dass neue und intelligente Technologien auch sicher und vertrauenswürdig sind, und so die nötige Akzeptanz finden werden.

Standpunkt 2

Die Betriebssicherheit (Safety) in der Industrie konsequent mit dem Schutz der digitalen Information (Security) bei IKT-Anwendungen vernetzen (Safety-and-Security-by-Design)! Aufbau geeigneter Sicherheitsarchitekturen in Unternehmen fördern!

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. So verfügen hochinnovative Produkte wie beispielsweise medizinische Geräte, zu denen u. a. Herzschrittmacher, Dialyse-Stationen und CT-Scanner gehören, über eigene IP-Adressen und eine integrierte Software, über die illegal durch das Ausnutzen von

Schwachstellen die Funktion des Produkts manipuliert werden kann. Gleiches trifft auch auf kritische Infrastrukturen, also neuralgische Systeme wie die Strom- und Wasserversorgung, zu.

Diese sind heute in Europa oft nicht ausreichend geschützt.

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 und der Vernetzungsgrad und die Datenflut weiter ansteigen, wächst auch die Verwundbarkeit der Anlagen durch Cyber-Attacken. Die konventionelle Betriebssicherheit (Safety) muss zukünftig konsequent in Interaktion zur Cyber Security als Gesamtbild verstanden und gemanagt werden. Im Mittelpunkt steht dabei der Aufbau geeigneter Sicherheitsarchitekturen der konventionell und digital vernetzten Produktionsprozesse. Das bedeutet, dass alle Aspekte der Sicherheit von Anfang an über die gesamte Wertschöpfungskette und den kompletten Lebenszyklus von Produkten, Systemen und der Software einbezogen werden müssen. Ziel muss es sein, sowohl die technische als auch die digitale Welt und ihr Zusammenspiel zu begreifen. Dann werden wir auch automatische Alarmierungs-, Analyse- und Auswertungsmöglichkeiten schaffen, so die Bedrohungen identifizieren, die Risiken bewerten und wirksame Schutzmaßnahmen ergreifen können.

Standpunkt 3

Rechtsvorschriften und Normen EU-weit harmonisieren!

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.

Wirksame Erkennungs- und Schutzkonzepte in Software-Anwendungen (App-Security) sind für Unternehmen und Organisationen wichtiger denn je. Um die Risiken zu minimieren und Schwachstellen zu beseitigen, bevor sie ein Hacker ausnutzen kann, sollte Security künftig ein wesentliches Leistungsmerkmal bereits 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.

Allerdings müssen auch komplexe IT-Systeme im Betrieb ständig auf ihre Sicherheit und aktuelle Schwachstellen überprüft werden, um daraus resultierende Risiken frühzeitig zu erkennen. Bisherige automatisierte Methoden haben sich für eine Risikoidentifikation häufig als unzureichend erwiesen, weil sie den Kontext der Anwendung nicht mit in die Betrachtung einbezogen. Intelligente neue Verfahren ermöglichen eine automatische Detektion, die zwischen Risiken und Schwachstellen unterscheidet und damit eine ressourcenschonende Priorisierung innerhalb des Schutzkonzepts zulassen. Die Methode lässt sich sowohl auf bereits in Betrieb genommene Applikationen als auch auf Software anwenden, die sich noch in der Entwicklung befindet.

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.

Standpunkt 4

Branchen- und EU-weite Technologiepartnerschaften sowie einen gemeinsamen europäischen Markt hierdurch ermöglichen!

Sicherheit in der digital vernetzten Welt kann nur durch Kooperation gewährleistet werden: Schulterschlüsse zwischen Nationen, enge Kooperationen mit Wirtschaft und Wissenschaft. Die Sicherheitsakteure sind gefordert, auf der Höhe der Zeit zu bleiben: Technische Voraussetzungen, geschultes Personal, rechtlich geeignete Rahmenbedingungen und hohe Anpassungsfähigkeit der Strafverfolgungsbehörden sind national und international durchgängig notwendig.

Die Verhandlungen zum Transatlantischen Handels- und Investitionspartnerschaftsabkommen (TTIP) müssen in Bezug auf IT-Sicherheit auf eine Stärkung des Sicherheitsniveaus für kommerzielle IT-Produkte abzielen. Dies betrifft im Besonderen das zentrale Element Kryptoalgorithmen.

Die Fähigkeiten und Qualifikationen im Bereich Cyber Security sind weltweit nicht gleichmäßig verteilt. Es wird in Zukunft darauf ankommen, dass die EU gemeinsam mit den EU-Mitgliedstaaten ihre Fähigkeiten im Bereich Cyber Security weiterentwickeln und weniger geschützte und sensibilisierte Regionen der Erde in der Bekämpfung von Cyber-Kriminalität zu unterstützen.