

PRESSEMITTEILUNG

System Security Engineering gewinnt an Bedeutung

Berlin, 24.11.2014 - Künftig wird System Security Engineering notwendig sein, um komplexe Systeme mit angemessenen Sicherheitseigenschaften ausstatten zu können. Darauf weist der Bundesverband IT-Sicherheit e.V. (TeleTrust) in einer aktuellen Veröffentlichung hin.

Einerseits werden IT-Systeme komplexer - dies zeigen viele Beispiele, wie vollautomatische Produktionsanlagen, elektronische Systeme in Fahrzeugen oder die Kommunikationsstrukturen, die dem Internet zugrunde liegen. Andererseits werden klassische Systeme zunehmend mit IT-Komponenten erweitert. Beispiel dafür sind Bauwerke, die mit einer Vielzahl von Sensoren ausgestattet werden, die permanent den Bauzustand dokumentieren. Damit wird das Bauwerk zu einem System, in dem auch IT-Sicherheit eine wichtige Rolle spielt.

Die frühzeitige Betrachtung von IT-Sicherheitsbelangen ist bei der Systementwicklung eine rechtliche und wirtschaftliche Notwendigkeit und nicht zuletzt immer häufiger eine Anforderung der Kunden.

Von Bedeutung ist dabei die Erkenntnis, dass es nicht ausreicht, die Sicherheitseigenschaften einzelner Komponenten zu überprüfen und sicherzustellen. Die Sicherheit eines Systems ist stets das Resultat des Zusammenwirkens vieler Komponenten an vielen Schnittstellen. Dieses Ergebnis ist oft überraschend anders als die Erwartung. Das gilt insbesondere für das Thema Systemsicherheit.

System Security Engineering liefert Konzepte, deren Anwendung es ermöglicht, Sicherheit zuverlässig in technische und technisch-organisatorische Systeme zu integrieren. Klassische Vorgehensweisen der Informationssicherheit wie die systematische Betrachtung von Bedrohungen, Schwachstellen und Anforderungen bis hin zur Risikoanalyse und der Ableitung von Maßnahmen werden gebündelt und gezielt auf den Lebenszyklus eines Systems sowie auf alle Komponenten und Schnittstellen angewendet. Dabei entstehen nicht unbedingt höhere Kosten, sondern es werden im Gegenteil zuverlässig Kosten eingespart, insbesondere was die Betriebsphase eines Systems angeht.

Mit einer jetzt vorgelegten Veröffentlichung leistet TeleTrust einen Beitrag zur aktuellen Diskussion über System Security Engineering. Das Dokument vermittelt die wichtigsten Inhalte sowie Anregungen für Systementwickler. Mit dem Personenzertifikat T.E.S.S. (TeleTrust Engineer for System Security) gibt TeleTrust Fachleuten die Möglichkeit, sich im Bereich System Security Engineering zu qualifizieren und sich diese Qualifikation von neutraler Stelle durch die prüfungsabnehmende Stelle PersCert TÜV bestätigen zu lassen.

TeleTrust-Publikation "System Security Engineering":

<https://www.teletrust.de/publikationen/broschueren/system-security-engineering/>

TeleTrust - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliedschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrust bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrust ist Träger der "TeleTrust European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrust Information Security Professional" (T.I.S.P.) und "TeleTrust Engineer for System Security" (T.E.S.S.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.