

PRESSEMITTEILUNG

Was ist "Stand der Technik" in der IT-Sicherheit? ENISA und TeleTrust - Bundesverband IT-Sicherheit e.V. veröffentlichen Handreichung in englischer Sprachfassung

Brüssel/Berlin, 07.02.2019 - In mehreren europäischen Ländern verfolgen die nationalen Gesetzgeber das Ziel, Defizite in der IT-Sicherheit abzubauen. Daneben gilt seit dem 25.05.2018 die EU-Datenschutz-Grundverordnung (DSGVO) mit ihren hohen Anforderungen an die technischen und organisatorischen Maßnahmen. Beide Rechtsquellen fordern die Orientierung der IT-Sicherheit am "Stand der Technik", lassen aber unbeantwortet, was im Detail darunter zu verstehen ist. In Deutschland haben die im Bundesverband IT-Sicherheit e.V. (TeleTrust) organisierten Fachkreise eine Handreichung erarbeitet, deren englische Sprachfassung in Kooperation mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) veröffentlicht wird.

Täglich zeigen Meldungen zu Sicherheitsvorfällen in Unternehmen und Behörden, dass dringender Handlungsbedarf zur Verbesserung der IT-Sicherheit besteht. Artikel 32 DSGVO regelt zur "Sicherheit der Verarbeitung", dass "unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen sind". Damit soll ein dem Risiko angemessenes Schutzniveau gewährleistet werden.

Sowohl die nationalen als auch der europäische Gesetzgeber enthalten sich jedoch konkreter, detaillierter technischer Anforderungen und Bewertungskriterien für die sicherheitsrelevanten technischen und organisatorischen Maßnahmen. Den Gesetzesadressaten werden auch keinerlei methodische Ansätze geliefert. Diese Ausgestaltung, zumal in einem dynamischen Marktumfeld, muss den Fachkreisen überlassen bleiben.

Das veröffentlichte Dokument zum "Stand der Technik" in der IT Security gibt vor diesem Hintergrund konkrete Hinweise und Handlungsempfehlungen. Die Handreichung soll Unternehmen, Anbietern und Dienstleistern Hilfestellung zur Bestimmung des Standes der Technik in der IT-Sicherheit geben und kann als Referenz z.B. für vertragliche Vereinbarungen, Vergabeverfahren bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen. Es ersetzt nicht eine technische, organisatorische oder rechtliche Beratung bzw. Bewertung im Einzelfall.

Durch die nun veröffentlichte englische Fassung des Dokumentes werden Unternehmen in allen europäischen Ländern bei der Bestimmung des geforderten Sicherheitsstands in der IT-Sicherheit unterstützt.

ENISA Executive Director Dr. Udo Helmbrecht: "Die Mitwirkung an diesem Handbuch ist Teil der Unterstützung, die ENISA für die EU-Mitgliedsstaaten leistet. Die Inhalte bieten konkrete Informationen und Empfehlungen, wie die IT-Sicherheit verbessert werden kann. Für IT-Experten ist die Handreichung eine nützliche Leitlinie, um in der Praxis den rechtlichen Anforderungen technisch gerecht zu werden."

TeleTrust-Vorsitzender Prof. Dr. Norbert Pohlmann: "Mit Hilfe der Bestimmung des Standes der Technik wird es uns gelingen, den Level an IT-Sicherheit angemessen zu erhöhen, unsere Robustheit gegen Cyber-Angriffe zu stärken und damit das Risiko der fortschreitenden Digitalisierung deutlich zu reduzieren."

TeleTrust-Vorstand RA Karsten U. Bartels: "Die Berücksichtigung des Stands der Technik ist eine technische, organisatorische und rechtliche Aufgabe für die Unternehmen und Behörden. Die Handreichung hilft auf diesen drei Ebenen sehr konkret - und das sowohl bei der operativen Umsetzung als auch bei deren Dokumentation."

Deutsche Version: <https://www.teletrust.de/publikationen/broschueren/stand-der-technik/>

Englische Version: <https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/>

ENISA - European Union Agency for Network and Information Security

Die Aufgabe der ENISA besteht darin, in der EU die erforderliche hochgradige Netz- und Informationssicherheit zu gewährleisten, indem sie einzelstaatlichen Behörden und den EU-Institutionen fachkundige Ratschläge zur Netz- und Informationssicherheit erteilt, als Forum für den Austausch bewährter Verfahren fungiert und Kontakte zwischen EU-Institutionen, staatlichen Behörden und Unternehmen erleichtert. Gemeinsam mit den EU-Institutionen und den staatlichen Behörden strebt die ENISA danach, eine Sicherheitskultur für EU-weite Informationsnetze zu entwickeln.

<https://www.enisa.europa.eu>

TeleTrust - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung 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 Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.