

PRESSEMITTEILUNG

Bundesverband IT-Sicherheit e.V. (TeleTrust): Schutz vor Cyberattacken auf Kritische Infrastrukturen und Industrie intensivieren

Gemeinsame Kraftanstrengung zu Verbesserung der IT-Sicherheit in Deutschland dringend erforderlich

Berlin, 24.03.2022 - Angesichts der veränderten geopolitischen Situation infolge des Ukraine-Konfliktes fordert der Bundesverband IT-Sicherheit (TeleTrust) von Politik, Regulierern und Betreibern weitreichende IT-Sicherheitsmaßnahmen und Investitionen zur Verbesserung der nationalen Sicherheit und der Versorgungssicherheit.

Cyberangriffe auf Unternehmen, staatliche Einrichtungen und kritische Infrastrukturen der Ukraine haben gezeigt, dass kritische Infrastrukturen und industrielle Netzwerke zunehmend in den Fokus politisch motivierter Cyberattacken geraten.

Energiewende und Digitalisierung der Produktion erfordern starke IT-Sicherheit

Die Beschleunigung der Energiewende und die zunehmende Vernetzung der Industrieproduktion einschließlich Logistik und Supply Chain erfordern zwingend ein hohes Maß an Digitalisierung und erhöht damit auch das Risiko, zu einem potentiellen Angriffsziel von politisch motivierten Hackern zu werden.

Steffen Heyde, secunet, Leiter der TeleTrust-AG "Smart Grids / Industrial Security": "Die neue geopolitische Lage, ausgelöst durch den Ukraine-Konflikt, ist Zäsur und Zeitenwende auch für die IT-Sicherheit in Deutschland. IT-Sicherheit ist ein entscheidender Pfeiler der nationalen Sicherheit und letztendlich Garant der Aufrechterhaltung von Versorgungssicherheit und des Funktionierens unserer Volkswirtschaft auch in Krisenzeiten."

Konzertierte Aktion zur Anhebung des IT-Sicherheitsniveaus erforderlich

TeleTrust fordert daher eine engagierte nationale Kraftanstrengung von Politik, Regulierern und Betreibern zur Verbesserung der Cybersicherheit und der nationalen Sicherheit:

- Beschleunigung der Energiewende und schnelle Digitalisierung mit einem sehr hohen Security Level;
- Nachschärfung des IT-Sicherheitsgesetzes auf ein höheres Sicherheits- und Vertrauensniveau;
- Strengere Prüfung der Umsetzung des höheren Sicherheitslevels durch Auditoren bei Versorgungsunternehmen (KRITIS);
- Pragmatische, unbürokratische Unterstützung und Förderung der KMUs bei der Bewältigung der IT-Sicherheitslage;
- Wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain;
- Beachtung der Vertrauenswürdigkeit von IT-Sicherheitslösungen bei Kaufentscheidungen;
- Verbesserung des Qualifizierungsniveaus des Personals in Bezug auf IT-/OT-Sicherheit.

Bundesverband IT-Sicherheit e.V. (TeleTrust)

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.