PRESSEMITTEILUNG

IT-Sicherheitsindustrie fordert spürbare Strafen bei Verwendung unsicherer IT

Unsichere IT stellt Sachmangel und Schlechtleistung dar

Konsequente Anwendung von Haftungsregelungen bei unsicherer IT

Moderne, zuverlässige IT-Sicherheitsmechanismen erforderlich

Ohne IT-Sicherheit keine nachhaltige Digitalisierung - und IT-Sicherheit kostet Geld

Berlin, 01.12.2016 - Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) fordert angesichts der jüngsten Hacker-Angriffe eine konsequente Anwendung bestehender Gesetze und Sanktionen für unzureichend gesicherte IT-Produkte. Es sei notwendig, dass flächendeckend auf die Sicherheit von Endgeräten geachtet werde.

"Wer andere gefährdet, in dem er schlecht gesicherte Geräte herstellt oder in Umlauf bringt, der muss dafür zur Verantwortung gezogen werden", fordert TeleTrusT-Vorstand Ammar Alkassar. Dies würde dazu führen, dass verstärkt Produkte verbreitet werden, die angemessen gesichert sind. "In einer zunehmend vernetzten Welt können wir uns unsichere Netzwerktechnik und Endgeräte nicht mehr erlauben."

Verantwortungsübernahme schließt Ersatz von nachgewiesenem Schaden als auch Bußgelder ein. Eine solche Regelung hätte überdies zur Folge, dass Unternehmen und Telekommunikationsanbieter verstärkt Zertifizierungen von den Herstellern verlangten, um sich selbst abzusichern. Der Sicherheitsstandard bei vernetzten Geräten und den damit betriebenen privaten oder öffentlichen Infrastrukturen würde dadurch steigen. "Die Fälle der letzten Zeit sind ein massiver Warnschuss", ergänzt Alkassar. "Wir müssen jetzt zügig handeln, denn die Zahl an internetfähigen Haushaltsgeräten, Geschäftsprozessen und kritischen Infrastrukturen steigt rapide an - und damit das Angriffspotential." TeleTrusT verweist in diesem Zusammenhang auf die Handreichung "Stand der Technik" (https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf).

TeleTrusT fordert neben rückhaltloser Aufklärung und Information, die Haftungsregelungen auf den Prüfstand zu stellen: Endkunden haben wenig Möglichkeiten, gegen große Anbieter empfindlich vorzugehen.

Das Problem betrifft sowohl das Verhältnis zwischen Anbieter und seinen Subunternehmen und Zulieferern als auch das Verhältnis zum Endkunden.

Neben der Regulierung durch den Staat sieht Alkassar, der auch Geschäftsführer des IT-Sicherheitsanbieters Rohde & Schwarz Cybersecurity ist, vor allem die IT-Sicherheitsbranche gefordert, umzudenken: "Wir müssen weg von Sicherheitssystemen, die den Angreifern hinterherrennen. Stattdessen brauchen wir proaktive Mechanismen, die Angriffe grundsätzlich verhindern." Zu erreichen sei dies beispielsweise durch die insbesondere von deutschen Anbietern favorisierte verstärkte Virtualisierung, Separierung und Datenflusskontrolle in IT-Systemen.

TeleTrusT - Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
www.teletrust.de