Verband der TÜV e.V.

TÜV®

Dezember 2017

VdTÜV-Position zum Verordnungsentwurf eines europäischen „Cybersecurity Acts“ vom 13. September 2017

Zehn Kernforderungen des VdTÜV

1. VdTÜV begrüßt, dass die Anforderungen an die Konformitätsbewertungsstellen dem „New Legislative Framework“ entsprechen. Zur Gewährleistung der Qualität der Prüfung und Zertifizierung dürfen ausschließlich akkreditierte Drittstellen zuständig sein. Dieses Zusammenspiel aus unabhängiger Konformitätsbewertung, Akkreditierung, Notifizierung und staatlicher Marktüberwachung dient einem effektiven und nachhaltigen Verbraucherschutz.
2. Die Vertrauenswürdigkeit eines Zertifikats ist an die Bewertung durch eine unabhängige Drittstelle gebunden. Produkte, Dienste, Prozesse und Systeme, die ein hohes Risiko aufweisen, müssen einer verpflichtenden Überprüfung durch unabhängige Dritte unterliegen.
3. Die Zertifikatsaussage muss stets höchstes Vertrauen verdienen. Sie sollte eindeutig, belastbar und transparent sein. Der Zertifizierung ist stets eine dem Risiko entsprechende Prüftiefe zugrunde zu legen. Je höher das Risiko, desto umfassender muss die Prüfung ausfallen.
4. Da wichtige Funktionen nicht mehr Bestandteil des IoT-Produktes sind („Back-End“-Systeme), müssen die Prüfungen über eine reine Produktbetrachtung hinausgehen.
5. Es bedarf einer Konkretisierung der Rollenverteilung. Wer prüft und zertifiziert, wer notifiziert und wer akkreditiert muss eindeutig festgelegt werden. Zur Vermeidung von Interessenkonflikten dürfen grundsätzlich die verschiedenen Akteure jeweils nur eine Rolle wahrnehmen. Ausnahmen müssen eindeutig definiert und eingegrenzt werden.
6. Ein Siegel muss konkret und einheitlich beschrieben werden und ein risikoadäquates Sicherheitsversprechen geben. Zertifizierung und die Siegelvergabe setzt voraus, dass ein akkreditierter Dritter die Bewertung durchgeführt hat. Zur Stärkung des Vertrauens sollte der Name des eingebundenen unabhängigen Dritten im Siegel enthalten sein. Die hinterlegten Prüfkriterien sollten in transparenter Weise öffentlich zugänglich sein.
7. Die zu erfüllenden Standards müssen ein hohes Maß an Vertrauen in die Sicherheit bieten. Die neue Rolle der ENISA darf nicht dazu führen, dass bestehende Standards ausgehöhlt werden. Etablierte hohe Standards (bspw. ISO/IEC 15408) müssen als Benchmark für ein europäisches Sicherheitsniveau gelten.
8. Die Interessengruppen müssen aufgrund ihrer Expertise und ihres Sachverstands intensiv bei der Erarbeitung der Zertifizierungsrahmen eingebunden werden.

9. Unabhängige Konformitätsbewertungsstellen benötigen zu Prüfungszwecken uneingeschränkten Zugriff auf die sicherheitsrelevante Steuerungstechnologie des Produktes oder Dienstes (und ihre Schnittstellen) unter Berücksichtigung hoher Datenschutzstandards.
10. Unabhängig vom Verordnungsentwurf müssen die produkt- und sektorspezifischen Anforderungen in den einzelnen „New Approach“-Regelungen in Bezug auf die Cybersicherheit überprüft und angepasst werden. Dabei bedarf es einer Neubewertung der Risiken. Zudem sollte der Aspekt der Robustheit von Produkten und der Interoperabilität in die Definition des allgemeinen Produktsicherheitsbegriffes integriert werden.