Beschluss der MU-Landesversammlung – Bayerischer Mittelstandstag vom 15. Oktober 2016 in Erlangen

Qualitätssiegel IT-Sicherheit – Offenlegung von IT-Schwachstellen

Die Bundesregierung soll das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) abändern und den Herstellern und Vertreibern von IT- Lösungen und IT-Produkten eine verbesserte Möglichkeit zur Meldung beim Bundesamt für Sicherheit in der Informationstechnik (BSI) schaffen.

Diesen soll erleichtert werden, Sicherheitslücken und konzeptionelle Schwächen gegenüber dem BSI offenzulegen, welches dann über die Publizierung im Sinne der Gefahrenabwehr und der voraussichtlichen Lösungszeit des Anbieters entscheidet.

Dazu soll ein Qualitätssiegel IT-Sicherheit geschaffen werden.

Begründung:

Ausgangssituation/Problemstellung

Gem. dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) sind die Betreiber kritischer IT Infrastrukturen dazu verpflichtet, entsprechende Sicherheitsüberprüfungen durchzuführen und z.B. Angriffe zu melden. Anbieter von IT-Lösungen entwickeln und verkaufen Produkte zum Zeitpunkt der Fertigstellung. Der Innovationsdruck und die Schnelligkeit der technischen Weiterentwicklung fordern ein regelmäßiges und schnelles Liefern. Während bei

agilen Entwicklungsmethoden und DevOps-Konzeptionen Unzulänglichkeiten eingeplant und durch kurzfristige Reaktionen kompensiert werden, sind bei fertigen Produkten auf dem Markt längere Update-Zyklen die Regel. Werden Sicherheitslücken oder konzeptionelle Schwächen entdeckt, so werden Kunden selten gewarnt, sondern meist über eine Anwendungsaktualisierung die möglichen Lücken behoben. Durch die Unkenntnis werden Anwendungen im produktiven Einsatz dann nicht aktualisiert und befinden sich dann langfristig ohne Risiko-Kenntnis des Unternehmens im Einsatz.

Durch eine Änderung des IT-Sicherheitsgesetzes würde den Unternehmen eine Handhabe gegeben, um die Risiken berücksichtigen zu können. Durch die Einbindung des BSI wäre die Vertraulichkeit und der vertrauensvolle Umgang mit sensiblen Sicherheits-Informationen gesichert. Eine verbesserte Möglichkeit zur Registrierung als Qualitätsmerkmal wäre insbesondere im Kontext von Einkauf und Angebotsstellungen für Verkäufer und Käufer hilfreich. Offenlegungen akuter Lücken und Schwächen können dann schnell und verantwortlich erfolgen, um den Nutzern selbst Möglichkeiten der Absicherung zu geben und eigene Risikoentscheidungen zu ermöglichen. Sogenannte Thread Infos oder relevante Vulns (Vulnerability/Schwachstelle) könnten dann für kritische IT-Systeme sichergestellt werden.

In letzter Zeit sind wiederholt Fälle bekannt geworden, in den IT-Sicherheitsprodukte selbst gravierende und vermeidbare Sicherheitsmängel hatten. Eine selbst angreifbare Sicherheitssoftware hat keine Schutzwirkung mehr, sondern vertieft Unsicherheit.

Lösungsskizze

Hersteller und Dienstleister der IT und der IT-Sicherheit sollten verbesserte Möglichkeiten erhalten, regelmäßige Sicherheitsprüfungen der angebotenen Softwarelösungen durchzuführen und dem BSI offen zu legen.

Das BSI könnte eine Liste von Herstellern herausgeben, die zusagen, für ihre Produkte die Schwachstellen an das BSI melden. Damit wäre dann eine Hilfestellung für die Unternehmen gegeben, die über das IT Sicherheitsgesetz verpflichtet sind. Zudem wäre es für die Anbieter eine Positiv-Werbung ihrer Angebote und Leistungen.

Das soll auch mit einem besonderen Qualitätssiegel IT-Sicherheit geschehen.