Bundesverband der Arzneimittel-Hersteller e.V. B.A.H

Stellungnahme

des Bundesverbands der Arzneimittelhersteller e.V.
zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme
Stand: 14.11.2014

Der Bundesverband der Arzneimittel-Hersteller e.V. (BAH) vertritt die Interessen der Arzneimittelindustrie gegenüber der Bundesregierung, dem Bundestag und dem Bundesrat. Mit seinen 467 Mitgliedsunternehmen, darunter 323 Arzneimittel-Hersteller, ist er der mitgliederstärkste Verband im Arzneimittelbereich. Die politische Interessenvertretung und die Betreuung der Mitglieder erstreckt sich zum einen auf den Bereich der Selbstmedikation, zum anderen auf das Gebiet der rezeptpflichtigen Arzneimittel mit Ausnahme der patentgeschützten Präparate.

Der BAH bedankt sich für die Möglichkeit, zu diesem Referentenentwurf Stellung zu nehmen und kommt der Bitte hiermit gerne nach.

Die Anmerkungen des BAH beziehen sich nachfolgend lediglich auf

Art. 1 des Gesetzentwurfs - Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnologie.

Allgemeiner Teil:

Grundsätzlich begrüßt und unterstützt der BAH die mit dem Gesetzentwurf intendierte Zielsetzung, gerade bei kritischen Infrastrukturen die Integrität und Authentizität datenverarbeitender Systeme und der für den Infrastrukturbetrieb notwendigen Netze zu schützen. Schon aus wirtschaftlichem Eigeninteresse ist heute jedes Unternehmen gefordert, sich mit den aktuellen sicherheitsrelevanten Herausforderungen der Informationstechnologie auseinandersetzen, um nicht durch externe informationstechnische Angriffe Betriebsausfälle und wirtschaftlichen Schaden für das Unternehmen selbst, aber auch für Dritte, hinnehmen zu müssen. Dies ist bereits heute tägliche Routinearbeit der in den IT-Abteilungen aller Unternehmen Beschäftigten.

Der BAH ist allerdings der Auffassung, dass es bereits jetzt eine Vielzahl von Regelungen gibt, die dieses Sicherheitsbedürfnis berücksichtigen, wie z.B. im Arzneimittelgesetz (AMG), der Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV), dem Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG), das Bundesdatenschutzgesetz (BDSG) und das Strafgesetzbuch (StGB), hier §§ 201 bis 210. Damit existieren bereits heute entsprechende rechtliche Rahmenbedingungen in Bezug auf die Sicherstellung der IT-Sicherheit und der Sicherstellung des Geschäftsbetriebs insbesondere von Arzneimittelherstellern. In diesen Vorschriften werden auch klare personelle Verantwortlichkeiten definiert.

Daher hält der BAH zusätzliche gesetzliche Regelungen für nicht erforderlich.

Er plädiert ferner dafür, dass jedes Unternehmen selbständig, im Rahmen des betrieblichen Risikomanagements, den Umfang der Sicherheitsvorkehrungen für die IT-Infrastruktur festlegt und kontinuierlich pflegt.

Ein solcher risikobasierter Ansatz findet sich im Übrigen auch in den - aus guten Gründen - streng regulierten Regelungen der Pharmakovigilanz, Arzneimittelherstellung und -prüfung. Hier werden konkrete Risiken identifiziert und priorisiert sowie entsprechend der Risikopriorität sukzessive umgesetzt.

Bislang betraf im Übrigen das Gesetz über das Bundesamt für Sicherheit in der Informationstechnologie bzw. die Zuständigkeit des Bundesamts (BSI) lediglich IT-Sicherheitsfragen von Bundesbehörden. Diese Zuständigkeit soll nun mit dem vorliegenden Gesetzentwurf umfänglich ausgeweitet werden. Es geht nunmehr auch im die Sicherheit datenverarbeitender Systeme Dritter, d.h. u.a. auch Unternehmen, die zu den sogenannten kritischen Infrastrukturen gehören. Welche Dritte damit genau gemeint sind, ist noch nicht klar. § 10 Abs. 1 (neu) des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnologie beinhaltet insofern eine Rechtsgrundlage für eine entsprechende Verordnung, die die kritischen Infrastrukturen nach § 2 Abs. 10 des Gesetzentwurfs bestimmen soll. Es wird im Gesetzentwurf selbst lediglich sehr unpräzise und allgemein aufgezählt, welche Sektoren darunter fallen, wie z.B. „Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen“. Welche Unternehmen aber genau darunter fallen, ist damit nicht klar. Insoweit ist der grundgesetzlich gesicherten Bestimmtheitsgrundsatz einer Rechtsgrundlage nicht Genüge getan.

Besonderer Teil:

Zu Art. 1 Ziff. 8 - § 8a Abs. 3 (neu):

Diese Regelung schreibt mindestens alle 2 Jahre die Durchführung von **Sicherheitsaudits** etc. durch anerkannte Auditoren sowie die Übermittlung die entsprechenden Berichte an das Bundesamt im gleichen Zeitintervall vor. Die Vorgabe von „mindestens alle 2 Jahre“ ist nach Auffassung des BAH nicht praxistauglich.

Es wird daher vorgeschlagen, diese Formulierung durch „regelmäßig“ zu ersetzen.

Des Weiteren wird auch an dieser Stelle noch einmal darauf hingewiesen, dass eine **differenzierte und insbesondere risikobasierte Betrachtung erforderlich** ist. Eine undifferenzierte Anwendung der vorgesehenen Regelungen auf alle Firmen einer Branche, unabhängig davon, ob es sich um sog. Global Player oder kleine und mittelständische Firmen handelt oder, ob eine Systemrelevanz vorliegt oder nicht ist nicht sachgerecht. Als Verband, der insbesondere auch klein- und mittelständische Unternehmen als Mitglieder hat, sehen wir mit großer Sorge, dass mit dem Entwurf ein weiterer zusätzlicher regulatorischer Aufwand auf diese Unternehmen zukommt, welche immer mehr Ressourcen für den laufenden Betrieb von EDV-Systemen abverlangen und damit zusätzliche Ressourcen binden, die eigentlich für die Weiterentwicklung des EDV-Betriebes und insbesondere auch für ihre Kernaufgabe, die Entwicklung und den Vertrieb von Arzneimitteln, vorgesehen sind.

Zu Art. 1 Ziffer 8 - § 8b Abs. 3

Die im Gesetzentwurf geforderte 24x7-Erreichbarkeit von IT-Sicherheitspersonal (Kontaktstelle als zuständiger Empfangspunkt Entscheidungsbefugnis) wird insbesondere in Unternehmen ohne 3-Schicht-Betrieb erheblich Personalzusatzkosten verursachen. Zusätzlich ist die im Gesetzentwurf nur grob skizzierte Kommunikationskette noch so konkret auszugestalten, dass diese kein neues potentielles informationstechnisch-sicherheitsrelevantes Einfallstor für potentielle Angreifer darstellt.

Wie bereits zuvor erläutert, werden bereits vorhandene Regelungen in anderen Bereichen, wie im Arzneimittelbereich, nicht berücksichtigt. Bereits jetzt müssen umfangreiche Validierungen und Audits für alle Teile der EDV vorgenommen werden, die im Umfeld der „Good Manufacturing Practice“ (GMP), „Good Manufacturing Distribution Practice“ (GMDP), „Good Laboratory Practice“ (GLP) und „Good Pharmacovigilance Practice“ (GVP) eingesetzt werden.

Dieser Gesetzentwurf wird im Besonderen für klein- und mittelständische Unternehmen zu enormen Mehrkosten führen. Um den formellen Teil derartiger Audits von Sicherheits-, Notfall- und IT-Risikomanagement-Plänen zu bestehen, hat eben nicht jedes klein- und mittelständische Unternehmen das formale Wissen. Daher werden entweder initial oder wahrscheinlicher dauerhaft teure Ressourcen in Form von externen Experten eingesetzt werden müssen. Da der Gesetzentwurf vorschreibt, dass lediglich Audits durch beim BSI zertifizierte Auditoren (und deren Zertifikat jeweils nur 3 Jahre gültig ist) valide sind, ist dieser Gesetzentwurf besonders für derartige Auditoren wirtschaftlich lukrativ, ohne hierdurch in der Praxis die IT-Sicherheit zu erhöhen. Lediglich die Kosten der unter erheblichem Kostendruck stehenden klein- und mittelständigen Arzneimittelhersteller werden dadurch erhöht werden.

Ein **branchenspezifischer IT-Sicherheits-Standard**, wie er dem Gesetzentwurf (auch unter Berücksichtigung der Tatsache, dass gem. § 8c immerhin Kleinstunternehmen ausgenommen sind.) zu entnehmen ist, ist daher nur sinnvoll, wenn dieser niedrig gehalten wird. Dann reicht der Standard aber für sensiblere Firmen nicht aus. Daher ist nicht unbedingt die Größe eines Unternehmens, sondern die „Systemrelevanz“ maßgebend bei der Frage, von welchem Sicherheitsstandard auszugehen ist. Diese Einstufung kann das Unternehmen am besten selbst vornehmen. Die Einstufung einer gesamten Gruppe „Gesundheit“ wird der Angelegenheit insofern nicht gerecht. Daher sollte nach Auffassung des BAH stärker differenziert werden, so dass nur solche Firmen in die Überwachung einbezogen werden, bei denen es aus übergeordneten, allgemeinen Interesse auch gerechtfertigt ist. Ein solches Vorgehen spart sowohl bei den Unternehmen der Branche als auch beim Staat Ressourcen und Kosten, ohne auf wesentliche Einschnitte bei der Sicherheit zu verzichten.

Insgesamt plädiert der BAH bei diesem Gesetzentwurf für eine risikobasierte Betrachtung mit Augenmaß, bei der auch bereits bestehende Regelungen in anderen (Spezial-)Gesetzen angemessene Berücksichtigung finden, damit das grundsätzlich begrüßenswerte Ziel angemessen erreicht werden kann.

Bonn, den 14.11.2014