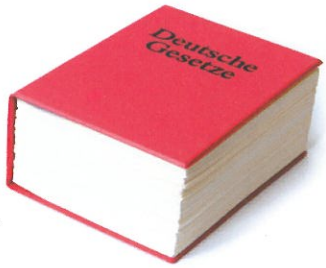
RECHTSTIPP |

Schutz vor Angriffen aus dem Netz gestärkt



Informationstechnik ist branchenübergreifend zu einem zentralen Bestandteil vieler Geschäftsprozesse geworden. Das neue IT-Sicherheitsgesetz soll für das Gemeinwesen existenziell wichtige Versorgungsstrukturen gegen Cyber-Attacken wappnen, wie Dr. Jonas Tritschler erläutert.

Jeder zweite deutsche Internetnutzer ist laut einer aktuellen Umfrage von TNS Emnid schon einmal Opfer von Cyberkriminalität geworden. Doch nicht nur Privatnutzer sind von dieser neuen Form der Kriminalität bedroht: Anfang 2015 erfolgte der bisher größte Cyberangriff auf den deutschen Bundestag. Von Cybercrime bedroht sind auch alle Unternehmen.

Um wichtige Versorgungsstrukturen für das Gemeinwesen vor Cyber-Attacken zu schützen, trat im Juli 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – kurz IT-Sicherheitsgesetz – in Kraft. Die Anpassung von insgesamt acht unterschiedlichen Gesetzen soll die Verbesserung der IT-Sicherheit bei Unternehmen, den Schutz der Bürger in einem sicheren Netz sowie den Schutz der IT des Bundes gewährleisten.

Betreiber Kritischer Infrastrukturen müssen nun IT-Sicherheitsvorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Schätzungsweise betrifft dies rund 2000 Betreiber. Dazu zählen IT-Infrastrukturen von Einrichtungen, die für das Gemeinwesen von hoher Bedeutung sind und deren Ausfall weitreichende Folgen haben würde. Dabei handelt es sich vor allem um Unternehmen aus den Bereichen Telekommunikation, Transport und Verkehr, Energie und Wasser, IT, Ernährung und Gesundheit sowie Finanzen und Versicherungen.

Künftig erfasst ein zentrales Meldesystem Informationen zu Beeinträchtigungen und Ausfällen von kritischen Infrastrukturen, die durch Cyberangriffe verursacht werden. Um die Sicherheit von IT-Produkten und -systemen für Kunden transparenter zu machen, soll das BSI zudem die Befugnis erhalten, auf dem Markt befindliche Produkte und Systeme im Hinblick auf ihre IT-Sicherheit zu prüfen, zu bewerten und die Ergebnisse bei Bedarf zu veröffentlichen.

Dr. Jonas Tritschler ist Geschäftsführer der FALK IT Consulting Services GmbH. Er ist Diplom-Wirtschaftsingenieur, Steuerberater, Wirtschaftsprüfer und Certified Information Systems Auditor (CISA).

Die Betreiber Kritischer Infrastrukturen sollen künftig verpflichtet sein, einen Mindeststandard an IT-Sicherheit einzuhalten. Angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse sind zu treffen, wobei der Stand der Technik maßgeblich ist.

Die Erfüllung der Anforderungen haben die Betreiber dem BSI mindestens alle zwei Jahre auf geeignete Weise nachzuweisen. Außerdem sollen die Betreiber Kritischer Infrastrukturen erhebliche IT-Sicherheitsvorfälle – oder sich andeutende – an das BSI melden. Die beim BSI zusammenlaufenden Informationen werden dort ausgewertet und den Betreibern Kritischer Infrastrukturen zur Verbesserung des Schutzes ihrer Infrastrukturen zur Verfügung gestellt.

Zur Steigerung der IT-Sicherheit im Internet werden darüber hinaus die Anforderungen an Diensteanbieter im Telekommunikations- und Telemedienbereich erhöht. Diese Pflichten richten sich dabei an alle Diensteanbieter, die kommerziell eine Internetseite betreiben, also nicht nur an Betreiber Kritischer Infrastrukturen. Alle Diensteanbieter sollen künftig Sicherheit nach dem jeweiligen Stand der Technik bieten. Telekommunikationsunternehmen werden zudem verpflichtet, ihre Kunden zu warnen, wenn auffällt, dass der Anschluss des Kunden, zum Beispiel im Rahmen eines sogenannten Botnetzes, für Angriffe missbraucht wird. Ziel ist es, einen der Hauptverbreitungswege von Schadsoftware einzudämmen: Hacker manipulieren fremde, unverdächtige Internetseiten, deren bloßer Besuch dazu ausreicht, anschließend im Hintergrund Schadsoftware auf dem Rechner des Besuchers zu installieren.

Praxistipp

Mit Inkrafttreten der Rechtsverordnung bleiben den Betreibern Kritischer Infrastrukturen maximal zwei Jahre, um entsprechende Maßnahmen umzusetzen. Dies mag nach viel Zeit klingen. Doch wer weiß, dass IT-Sicherheitsprojekte sehr oft grundlegende Veränderungen der System- und Softwarearchitektur erfordern, wird sehr schnell Handlungsmaßnahmen ableiten müssen, um den Anforderungen des Gesetzes im Rahmen der zeitlichen Vorgaben gerecht zu werden.