knipp

Handlungsbedarf für Unternehmen durch IT-Sicherheitsgesetz

Neue Sicherheitsauflagen für Kritische Infrastrukturen

Bereits im Juli 2015 ist in Deutschland ein IT-Sicherheitsgesetz in Kraft getreten, das den Schutz der heimischen IT-Infrastrukturen verbessern soll. Viele Telekommunikationsanbieter und Betreiber von Webservern oder Online-Shops wissen jedoch gar nicht, dass sie seitdem erhöhte Auflagen zum Schutz von Kundendaten und IT-Systemen erfüllen müssen.

Voraussichtlich Anfang Mai 2016 wird dieses IT-Sicherheitsgesetz nun um eine Rechtsverordnung ergänzt, die die Regelungen auf alle für die Versorgung der Allgemeinheit wichtigen Bereiche erweitert. Das betrifft zunächst die sogenannten Kritischen Infrastrukturen in den Bereichen Informationstechnik und Telekommunikation, Energie, Wasser und Ernährung. Bis Anfang 2017 sollen dann noch die Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen folgen.

Die Betreiber der betroffenen Anlagen und Dienstleistungen sind verpflichtet, innerhalb von sechs Monaten eine zentrale Kontaktstelle zum Bundesamt für Sicherheit in der Informationstechnik (BSI) einzurichten und innerhalb von zwei Jahren die Einhaltung eines Mindeststandards an IT-Sicherheit nachzuweisen. Zudem gelten Meldepflichten für sicherheitsrelevante Vorfälle wie Cyber-Attacken, Phishing oder IT-basierte Erpressungsversuche. Ziel dieser Meldepflicht ist es, ein aktuelles Bild über die

Gefährdungslage der Cyber-Sicherheit in Deutschland zu bekommen und entsprechende Präventions- und Gegenmaßnahmen planen zu können.

Wer als Betreiber einer Kritischen Infrastruktur im Sinne des Gesetzes gilt, wird in der BSI-Kritis-verordnung (KritisV) durch einen Kriterienkatalog festgelegt. Für die dem Internet zugrunde liegenden DNS-Dienste beispielsweise wird unter anderem die Anzahl der abgefragten IP-Adressen pro Tag betrachtet. Allerdings sind die Betreiber selbst in der Pflicht, den Versorgungsgrad Ihrer Anlagen zu bestimmen und festzustellen, ob sie als Kritische Infrastruktur gelten. Das Problem dabei ist, dass sich viele Betroffene dieser Verpflichtung und den möglichen Konsequenzen gar nicht bewusst sind. Denn es drohen Bußgelder von bis zu 100.000 Euro, wenn die vorgeschriebenen Maßnahmen zur Vermeidung von Störungen nicht angemessen umgesetzt werden oder wenn Sicherheitsvorfälle nicht ordnungsgemäß oder verspätet gemeldet werden.

Aus diesem Grund sollte jedes Unternehmen, das in einem der genannten Sektoren tätig ist, den in der Verordnung festgelegten Kriterienkatalog prüfen. Die Zeit für die Umsetzung der Richtlinien könnte sonst knapp werden.

Eine einfache und verständliche Möglichkeit um festzustellen, ob man als Betreiber einer Kritischen Infrastruktur eingestuft wird, bietet der »Online-Test Kritische Infrastruktur«. Dabei handelt es sich um einen interaktiven Fragebogen, den der DNS-Spezialist ironDNS unter https://irondns.net/kritisv bereit hält. Dort gibt es außerdem kurze

und verständliche Erläuterungen, Hinweise zu möglichen nächsten Schritten und weiterführende Informationen.

Link zum »Online-Test Kritische Infrastruktur«:

https://irondns.net/kritisv

Über ironDNS

ironDNS ist eine Premium DNS-Dienstleistung für Internet-Domains mit speziellen Anforderungen an Betriebssicherheit und weltweiter, schneller und zuverlässiger Erreichbarkeit.

ironDNS ermöglicht den Betrieb von kritischen DNS-Infrastrukturen auf höchstem technischen Niveau. Eingebettet in ISO 27001-zertifizierte Prozesse erfüllt ironDNS alle nach dem IT-Sicherheitsgesetz geforderten Auflagen schon heute.

ironDNS ist eine Dienstleistung der in Dortmund ansässigen Knipp Medien und Kommunikation GmbH.

(Diese Meldung besteht aus 3.094 Zeichen bzw. 401 Wörtern.)

Knipp Medien und Kommunikation GmbH
Martin-Schmeißer-Weg 9
Technologiepark
44227 Dortmund
Telefon +49 231 9703-0
Fax: +49 231 9703-200
Presse-URL: http://www.knipp.de/go/presse
Ansprechpartner: Linda Müller
E-Mail: Linda.Mueller@knipp.de