IT-Sicherheitsgesetz: Bürde oder Chance für Unternehmen?

Kommentar von René Leitz, Teamleiter Product Development bei der G+H Systems GmbH

Das viel diskutierte IT-Sicherheitsgesetz trat am 25.07.2015 in Kraft – und wirft einige Fragen auf. Welche Unternehmen betrifft das Gesetz? Welche Sicherheitsstandards müssen erfüllt werden? Deutsche Firmen sind verunsichert bzw. haben Bedenken, ob sie den Anforderungen des Staates genügen können. Dabei soll das Gesetz doch vor allem eines: aufmerksam machen!

Die deutsche Bundesregierung führt mit dem IT-Sicherheitsgesetz erstmals offizielle Regularien ein, die Firmen aus der Wirtschaft (gemäß Rechtsverordnung nach § 10 Abs. 1 BSIG) dazu verpflichten, spätestens zwei Jahre nach einem gemeldeten IT-Sicherheitsvorfall „angemessene organisatorische und technische Vorkehrungen“ zur Vermeidung eines solchen Ereignisses zu treffen bzw. einzuführen.

Für mich sowie für die Firmen selbst ist allerdings unklar, an wen sich dieses neue Gesetz genau richtet? Der Gesetzesschrift zufolge geht es grundsätzlich um die „Betreiber besonders gefährdeter Infrastrukturen“, sogenannter „kritischer Infrastrukturen“. Folgende Sektoren sind hiermit angesprochen: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. So weit, so gut!

Geht es noch konkreter? Leider nein, das Gesetz definiert kritische Infrastrukturen nur abstrakt. Daher sollen aktuell eigene Rechtsverordnungen für jede relevante Branche erstellt werden, um klar zu bestimmen, welches Unternehmen unter das IT-Sicherheitsgesetz fällt. Denn die Firmen müssen sich zukünftig an gewisse „Mindeststandards für die IT-Sicherheit“ halten. Diese Standards werden branchenweit festgelegt und von den Unternehmen selbst entwickelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) entscheidet, ob die eigens kreierten Standards genehmigt werden oder nicht. Im Anschluss findet spätestens alle zwei Jahre eine Prüfung statt, ob die standardisierten Sicherheitsmaßnahmen eingehalten werden. Bei den Mindeststandards ist die Rede ist von „Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen maßgeblich sind".

Chance: Unternehmen werden wachgerüttelt

Schon während des Lesens der fast schon einschüchternden Gesetzestexte wird deutlich, dass die Unternehmen ohne Zweifel vor einer großen Herausforderung stehen. Aber warum müssen Firmen vom Staat dazu „gezwungen“ werden, mehr Wert auf ihre IT-Sicherheit zu legen? Haben die Verantwortlichen selbst kein Interesse daran? Auf diese Fragen werden wir wohl keine zufriedenstellenden Antworten erhalten.

Doch wenn ich diese Fragen einmal beiseitelege, sehe ich das neue Gesetz vor allem als sehr große Chance. Unternehmen werden nun öffentlich darauf aufmerksam gemacht, ihre IT-Infrastruktur endlich besser abzusichern. Firmen sollen investieren. Der Fokus liegt dabei auf der Prävention. Größere Schäden wie z.B. Betriebsspionage können vermieden werden; keine Chance mehr für Datendiebstahl und ähnliche Delikte.

Ich bin der Meinung, dass dieser vorbeugende Ansatz für Unternehmen besser ist als die ansonsten üblichen forensischen Analysen oder Echtzeitüberprüfungen des Netzwerks. Solche reaktiven Vorgänge decken nur das auf, was bereits passiert ist – ein teilweise irreparabler Schaden für die Firma. Daher empfehle ich, Mechanismen einzubinden, die aktiven Schutz ermöglichen. Nur so sichern Unternehmen ihre Infrastruktur langfristig ab und handeln stets im Sinne des neuen IT-Sicherheitsgesetzes.

Zum Autor:
René Leitz ist als Teamleiter Product Development bei der G+H Systems GmbH in Offenbach tätig. Das Unternehmen ist unter anderem im Bereich der Berechtigungsanalyse aktiv – einem sehr sensiblen und für Schwachstellen anfälligen Feld der Firmen-IT. Durch Access Governance-Tools ermöglicht G+H, potenzielle Risiken bzw. Angriffsflächen im Umfeld der Berechtigungszuweisungen von vornherein zu reduzieren oder gar zu eliminieren.