securitymanager.de
Das IT-Security Portal

Relevanz von IT-Sicherheit - theoretisch erkannt, praktisch vernachlässigt

http://www.securitymanager.de/magazin/news_h21099_relevanz_von_it-sicherheit_-_theoretisch.html

Ohne Computer und Internet funktioniert heutzutage nichts mehr, insbesondere im Arbeitsleben. Weitgehend sind die damit verbundenen Bedrohungen aus dem Internet, aber auch durch unachtsames Verhalten von Anwendern, Sicherheitslücken und -mängeln in der Organisation bis hin zu böswilligen Attacken auf Computersysteme bekannt. Warum reagieren Unternehmen dann erst nach einem Schadensfall? Diese Frage stellt sich der Datenschutzexperte Harald Pultar aus Mainz.

Vielen Anwendern ist zwar die Bedeutung von IT-Sicherheit theoretisch klar, in der Praxis fehlt es jedoch weitgehend an deren Umsetzung und Kontrolle. Wie das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinem Bericht zur Lage der IT-Sicherheit in Deutschland feststellt, wird das Thema erst nach einem Schadensfall wahrgenommen, obgleich der wirtschaftliche Erfolg maßgeblich von einer funktionierenden IT abhängt.

Wie eine Umfrage von GULP - das Portal für IT-Projekte und Marktführer in der Besetzung von IT-Projekten mit externem Personal zeigt, wird das Thema IT-Sicherheit von Projektanbietern und IT-Freiberuflern als sehr bedeutend eingestuft. Nach einer repräsentativen Studie des BSI haben rund 83 Prozent der befragten Wirtschaftsunternehmen das Thema IT-Sicherheit auf Platz eins oder zwei ihrer Prioritätenliste gesetzt.

"In der Praxis zeigt sich jedoch eine große Diskrepanz zwischen Anspruch und Umsetzung", weiß Pultar. Während bei Großunternehmen die Sicherheits-Budgets laut Studie von CIO, CSO und PricewaterhouseCoopers um durchschnittlich 17 Prozent steigen, deckt eine Untersuchung durch Checkpoints noch große Lücken gerade im deutschen Mittelstand auf. "Hiernach hat etwa die Hälfte der Unternehmen keinen Datenschutzbeauftragten und etwa 40 Prozent keinerlei Maßnahmen ergriffen, Mitarbeiter über Risiken aufzuklären, entsprechend zu schulen sowie Regeln im Umgang mit der IT aufzustellen und zu kontrollieren", so der Datenschutzexperte weiter.

Da es noch kein kodifiziertes Recht der IT-Sicherheit gibt, müssen Haftungsfragen vor Gericht stets im Einzelfall entschieden werden - die Rechtsprechung wird auf Grund von Präjudizien weiterentwickelt. Ob ein Unternehmen fahrlässig gehandelt oder die notwendige Sorgfalt vermissen lässt, wird neben Sachverständigen, Standards und branchenüblichen Maßnahmen auch durch die Awareness-Aktivität des Unternehmens beurteilt. "Dabei könnte sich die Mitarbeitersensibilisierung und die Erfüllung der klaren Vorgaben der im Anhang zu § 9 Bundesdatenschutzgesetz definierten sieben Kontrollpflichten wie Zutritts- und Zugriffskontrolle eher auszahlen, als reine Technikdetails", gibt Pultar zu Bedenken.

17.11.2006, EDV-Beratung PULTAR GmbH