Vorwort

Das unbekannte Unbekannte

> *There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know.*

In einem anderen Zusammenhang und zu einer anderen Zeit hat Donald Rumsfeld das obige Zitat geprägt. Es ging ihm um die Darstellung verschiedener Sichten auf die Gefährdung der nationalen Sicherheit durch Dritte. Die Einsicht und die Deutungen, die dahinterstecken, ähneln sehr stark auch den Themen, mit denen wir uns im Folgenden beschäftigen werden.

Auf den Themenkomplex IT-Sicherheit übertragen, lässt sich der Inhalt des Zitats folgendermaßen interpretieren: Es gibt Bedrohungen, von denen wissen wir, dass sie existieren und wo sie zu suchen sind. Diesen Bedrohungen nicht augenblicklich nachzugehen, wäre fahrlässig. Mit Regelungen und eingeübten Prozessen kann man die Risiken, die damit verbunden sind, in den Griff bekommen. Es gibt aber auch Bedrohungen, von denen wir wissen, dass sie existieren könnten, es fällt uns allerdings schwer, sie immer rechtzeitig zu verorten, und damit ist der Aufwand, Gegenmaßnahmen zu ergreifen, entsprechend höher und die Prozesse, die erforderlich sind, die entsprechenden Risiken unter Kontrolle zu halten, sind zunehmend komplexer. Am gefährlichsten ist aber die dritte Art an Bedrohungen: Dabei handelt es sich um diejenigen, von denen wir überhaupt nicht wissen, dass sie existieren.

Die Schlussfolgerung aus dieser Definition ist ernüchternd: Je weniger ausgeprägt das Sicherheitsniveau eines Unternehmens ist, desto mehr Bedrohungen wird es geben, die in die dritte, die gefährlichste, Kategorie fallen. Man wird einfach nicht wissen, welche Gefährdungen es gibt und an welcher Stelle diese auftauchen. Das führt so weit, dass selbst, wenn man bereits erfolgreich angegriffen wurde, man dies nicht bemerken wird, schlicht deshalb, weil man nicht darauf achtet. Das Verheerende daran ist, dass je weniger ein Unterneh-

men über die Bedrohungen weiß, denen es ausgesetzt ist, desto weniger stark wird auch das Bedürfnis sein, sich dagegen zu schützen. Mit einem steigenden Bewusstsein für die Risiken wird auch die Nachfrage nach Transparenz steigen und erst mit dieser wird ersichtlich, was bis dahin im Verborgenen lag. Denn Fakt ist: Der Abfluss an Know-how betrifft jedes Unternehmen jedweder Größe. Was Unternehmen jeweils voneinander unterscheidet, ist die Ausprägung und eventuell die Art und Weise, wie es geschieht, und natürlich der Umgang mit dieser Tatsache.

Bevor es losgeht

Das Ziel des Buches ist es, ein Projekt aufzuzeigen, das das Ziel hat, ein akzeptables Sicherheitsniveau in einem mittelgroßen Unternehmen zu erreichen. Das Projekt wird in drei Phasen, in unserem Fall »Schritte« genannt, untergliedert, hat klar definierte Aufgaben und Bereiche und soll am Ende nur drei Monate dauern. Ganz offensichtlich ist das ein Ansatz der anspruchsvolleren Art. Aber im Grunde ist es auch eine Notwendigkeit, denn viel mehr Zeit und Aufwand darf es einfach nicht kosten, weithin erprobte Regeln, Maßnahmen und Prozesse in einem durchschnittlich strukturiert aufgestellten Unternehmen einzuführen.

Durch die Bereitstellung einfacher Werkzeuge und der Begleitung bei stark vereinfachten Projektschritten soll es gelingen, Sicherheit auch dorthin zu bringen, wo sie bislang nur eingeschränkt gelebt wird. Eingeschränkt bedeutet in diesem Fall so viel wie »lückenhaft« und genau an diesen offenen Flanken setzen Angreifer am liebsten an, um Daten zu entwenden oder IT-Systeme zu sabotieren.

Hinweis

In Anlehnung an die 70:30-Regel geht es in der IT-Sicherheit nicht darum, 70 % der Sicherheitsfelder zu 100 % abzudecken, sondern darum, 100 % der Bereiche abzudecken, und zwar zu einem Niveau, bei dem man guten Gewissens noch gut schlafen kann. Das wiederum kann dann 80 % oder auch 70 % von theoretisch möglichen 100 % bedeuten. Ein flächendeckendes, einheitlich hohes bis sehr hohes, also akzeptables Niveau, an IT-Sicherheit ist damit das Ziel.