

Teil V

Incident Response – Reaktion und Wieder- herstellung



Häufig werden die Maßnahmen zur Sicherheit von Rechnern und Netzwerken wie eine simple Liste von den Unternehmen abgearbeitet. Hierbei erhalten die entsprechenden Punkte dieser Liste einmalig eine gewisse Aufmerksamkeit. Bestimmte Lösungen werden implementiert und der Punkt auf der Liste abgehakt. Anschließend wenden sich die Unternehmen wieder anderen scheinbar wichtigeren Aufgaben zu.

Die Unternehmen gehen davon aus, dass 100% Sicherheit gegeben ist, sobald die entsprechenden Maßnahmen getroffen wurden. Leider wird viel zu häufig verkannt, dass Sicherheit kaum messbar ist.¹ Sicherheit ist ein Prozess und muss ständig gepflegt werden. Hierzu ist es erforder-

1 Gibt es 90% Sicherheit? Was sind 90% Sicherheit? Jeder zehnte Angreifer ist erfolgreich!

lich, dass im Vorfeld bereits gewisse Vorbereitungen getroffen wurden und ständig die eingerichteten Lösungen überwacht werden. Ein wesentlicher Punkt bei einem Sicherheitskonzept ist die *Incident Response*. Hiermit bezeichnet man die Reaktion auf einen unerlaubten Vorgang.

Die erfolgreiche Incident Response erfordert eine genaue Planung im Vorfeld. Eine effektive Incident Response-Planung ist vergleichbar mit der Planung für den Fall eines Feuerausbruches. Die Incident Response, die Reaktion auf den Vorfall, ist vergleichbar mit der Brandbekämpfung.