Die Angriffsspuren sichtbar machen

Bild: adimas – Fotolia

Betreiber kritischer Infrastrukturen müssen Zwischenfälle bei der IT-Sicherheit melden. Ein spezielles Informationssystem kann sie dabei unterstützen. VON ARMIN MÜLLER

Nach dem IT-Sicherheitsgesetz müssen die Betreiber kritischer Infrastrukturen, zu denen auch Energieversorger zählen, mit organisatorischen und technischen Mitteln dafür sorgen, dass das geforderte Niveau an IT-Sicherheit eingehalten wird. Dem dient die Einführung eines Information Security Management Systems (ISMS), das bis Ende 2017 in den Unternehmen aufgebaut und zertifiziert sein muss.

Die Unternehmensberatung für Informationssicherheit ConSecur aus Meppen macht jetzt auf eine weitere Pflicht aufmerksam, die sich für Energieversorger aus dem IT-Sicherheitsgesetz ergibt. In § 8b des Gesetzes ist festlegt, dass „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen führen können“ dem Bundesamt für Sicherheit in der Informationstechnik zu melden sind. Wer Störungen bekanntgeben möchte, muss zunächst kritische Vorfälle erkennen, bewerten und dokumentieren. Dafür gibt es ein Security Information and Event Management System (SIEM), das die Aktivitäten in der IT-Landschaft sichtbar macht und sie nach Angriffsspuren durchsucht. Das System sammelt von den Netzkomponenten wie Router und Firewalls, den IT-Systemen und Anwendungen die Protokolldaten, die so genannten Logs, ein, wertet diese aus und schlägt Alarm, sobald eine verdächtige Kombination von Ereignissen erkannt wird. Es kann dabei helfen, das Ausmaß von Störungen zu reduzieren, indem ein Vorfall schnellstmöglich erkannt wird und Gegenmaßnahmen eingeleitet werden können. Die Berater von ConSecur empfehlen den Unternehmen, in einem ersten Schritt herauszufinden, welche Daten und welche IT-Funktionen als kritisch im Sinne des IT-Sicherheitsgesetzes zu bewerten sind. Es könne aber nicht schaden, in die Betrachtung auch die kritischen Geschäftskomponenten eines Unternehmens einzubeziehen, die nicht vom IT-Sicherheitsgesetz genannt werden.

Schon heute versuchen Unternehmen, ihre Daten durch eine effiziente IT-Sicherheitsarchitektur zu schützen. Eingesetzt werden beispielsweise Anti-Viren-Systeme, Firewalls, ein Zugriffsschutz oder Rollenkonzepte, die Berechtigungen verteilen und verwalten. Diese Maßnahmen schützen allerdings in der Regel nicht lückenlos. Einerseits entwickeln die Angreifer immer neue Methoden, andererseits ist eine wesentliche Schwachstelle bei der IT-Sicherheit oft der Mitarbeiter, dessen Fehler, etwa beim Öffnen eines infizierten Mail-Anhangs, als Einfallstor in das Unternehmen genutzt werden.

Protokolle helfen bei den Nachweisen

Ein SIEM-System kann hier den Schaden begrenzen, denn es zeichnet alle Ereignisse, die Hinweise auf Angriffe geben, auf und wertet sie aus. So kann es beispielsweise passieren, dass eine Anti-Viren-Software einen Angriff nicht entdeckt, weil für den Schädling noch keine Signatur vorliegt. Doch die Schadsoftware erzeugt Spuren: Damit sie weiß, was sie auf dem Rechner tun soll, kommuniziert sie mit einem Server im Internet. Diese Kommunikation zeichnet die Firewall auf und sendet das Ereignis an das SIEM. Dieses stellt dann anhand einer Liste bekannter Server fest, dass der Ziel-Server „böse“ ist und schlägt Alarm und es können geeignete Gegenmaßnahmen eingeleitet werden.

Zugleich hilft das System auch bei dem Erstellen von Nachweisen, die das IT-Sicherheitsgesetz von den Betreibern kritischer Infrastrukturen fordert. Denn alle beobachteten Aktivitäten werden protokolliert und sind dann auf Knopfdruck für aktuelle Sicherheitsreports und diverse Audits verfügbar. Ein SIEM-System unterstützt so das Information Security Management System dabei, regelbasiert und kontinuierlich die Standards für Sicherheit, Compliance und Qualität des IT-Betriebs sicherzustellen und zu verbessern. E&M