DEUTSCHES IT-SICHERHEITSGESETZ

Inhalt und Compliance

ANFORDERUNGEN

Seit 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft. Hierdurch soll eine signifikante Verbesserung der IT-Sicherheit in Deutschland erreicht werden. Betreiber sog. „kritischer Infrastrukturen" müssen wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer IT-Infrastrukturen nach sich ziehen kann, ein Mindestniveau an IT-Sicherheit einhalten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsvorfälle melden. Unter „kritischen Infrastrukturen" werden Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen verstanden, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die kritischen Infrastrukturen werden durch eine noch zu erlassende Rechtsverordnung näher bestimmt.

Betreiber kritischer Infrastrukturen müssen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen. Dabei soll der Stand der Technik eingehalten werden. Die Unternehmen haben eine Übergangsfrist von zwei Jahren nach Inkrafttreten der Rechtsverordnung. Bis dahin müssen sie u.a. sicherstellen, dass sie branchenspezifische Mindestanforderungen an die IT-Sicherheit erfüllen, wie Maßnahmen zur Erkennung (Detektion) und Behebung von Störungen, Einrichten eines Information Security Management, Identifizierung kritischer Cyber-Assets, Maßnahmen zur Angriffsprävention und -erkennung und Implementierung eines Business Continuity Managements. Die Betreiber kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Bei Sicherheitsmängeln kann das BSI die Audit-, Prüfungs- oder Zertifizierungsergebnisse anfordern und die Beseitigung der Sicherheitsmängel anordnen.

Zudem werden Betreiber kritischer Infrastrukturen durch das IT-Sicherheitsgesetz verpflichtet, erhebliche Störungen ihrer IT-Systeme, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit führen können oder geführt haben, an das BSI zu melden. Das BSI kann unter bestimmten engen Voraussetzungen Informationen über Störungen öffentlich machen, so dass hierdurch auch die Reputation des betroffenen Unternehmens leiden kann.

Verstöße gegen das IT-Sicherheitsgesetz können mit Geldbußen bis zu 100.000 Euro geahndet werden. Lediglich Kleinstunternehmen sind von den Verpflichtungen ausgenommen.

Durch das IT-Sicherheitsgesetz werden zudem Diensteanbieter von Telemedien wie etwa Betreiber werbefinanzierter Webseiten verpflichtet, im Rahmen des technisch Möglichen und wirtschaftlich Zumutbaren sicherzustellen, dass kein unerlaubter Zugriff auf ihre technischen Einrichtungen möglich ist und diese gegen Datenschutzverletzungen und äußere Angriffe gesichert sind. Wesentliches Ziel der Regelung ist es, die Verbreitung von Schadsoftware einzudämmen, und die Diensteanbieter haben entsprechende organisatorische Vorkehrungen zu treffen, wie etwa den Einsatz von Virenscannern und das Einspielen regelmäßiger Sicherheitspatches ihrer Software. Das Gesetz sieht ausdrücklich vor, dass eine Maßnahme hierunter insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens ist.

Trend Micro unterstützt seine Kunden bei der Einhaltung der Anforderungen des IT Sicherheitsgesetzes.

TREND MICRO DEEP SECURITY:

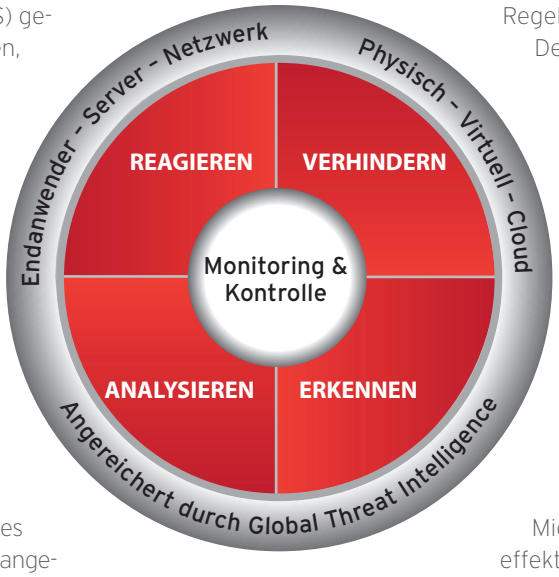
Deep Security wurde speziell unter dem Gesichtspunkt der Einhaltung von gesetzlichen bzw. branchenspezifischen Vorschriften (Compliance) in der IT entwickelt. Die Lösung unterstützt Unternehmen bei der Einrichtung eines Information Security Management Systems (ISMS), das die Verfahren und Regeln innerhalb einer Organisation definiert. Deep Security bietet eine Fülle vordefinierter Security Policies, aber auch die Möglichkeit, diese individuell zu konfigurieren und eigenen Vorgaben anzupassen.

Als Teil eines ISMS vereint die Lösung, wie vom IT-Sicherheitsgesetz gefordert, klassische Präventivmaßnahmen (wie beispielsweise IDS/IPS) gegen Angriffe mit Monitoring-Funktionen, die einerseits existierende Schwachstellen in der Infrastruktur wie auch ungewöhnliche Zugriffe erkennen und abstellen können.

Zur Angriffsprävention zählt nicht zuletzt das Patching, und zwar zeitnah. Die Erfahrung lehrt jedoch, dass die IT-Abteilungen dieser Anforderung in vielen Fällen nur schwer nachkommen können. Mit Deep Security erfüllen Unternehmen dennoch die Anforderungen des IT-Sicherheitsgesetzes ohne dabei den Betrieb ihrer kritischen Systeme unterbrechen zu müssen, denn virtuelle Patches schirmen Schwachstellen ab, bevor sie angegriffen werden können, und schützen vor Exploits.

Eine ausführliche und dafür angepasste Reporting-Funktion unterstützt die IT-Abteilungen bei der Zusammenstellung von für Audits relevanten Informationen (z.B. Change Management). Die Lösung kann ebenfalls problemlos Systeme in Cloud Umgebungen einbinden und hier dieselben Sicherheitsmaßnahmen implementieren, die Unternehmen aus dem heimischen Netzwerk gewohnt sind. Die Zusammenführung aller Daten in einer zentralen Managementeinheit ermöglicht es den Betreibern, jederzeit einen Überblick über aktuelle Risiken in der zu schützenden Umgebung zu erhalten.

Weitere Informationen finden Sie unter:
www.trendmicro.de/deep-security



TREND MICRO DEEP DISCOVERY:

Heutige Präventivmaßnahmen müssen zusätzlich zum Schutz vor bekannten Bedrohungen auch eine Verteidigungslinie gegen unbekannte Bedrohungen, wie etwa gezielte Angriffe, umfassen, für die es noch keine Muster oder Regeln gibt. Während die meisten Unternehmen bereits in Schutzmaßnahmen wie Antivirus investiert haben, fordert der Gesetzgeber explizit Maßnahmen zur Erkennung (Detektion) und diese am „Stand der Technik" auszurichten. Das bedeutet aber, dass er auch Maßnahmen fordert, die sich auf Bedrohungen beziehen, für die es noch keine Muster oder Regeln gibt.

Deep Discovery unterstützt Anwender in diesen Fällen, denn die Lösung besteht aus Technologie, die bewußt für noch nicht bekannte Bedrohungen entwickelt wurde, und daher immer den „Stand der Technik" repräsentiert.

Das Produkt gehört zur Klasse der sogenannten „Breach Detection Systeme", die vor allem unbekannte Muster aufdecken sollen, um auch getarnte Angriffe zu bekämpfen. In einem unabhängigem Test solcher Systeme bescheinigte das Testinstitut NSS Labs der Trend Micro Lösung eine hohe Sicherheitseffektivität sowie das Prädikat „empfohlen" (recommended).

Sie ermöglicht die rasche Erkennung von ungewöhnlichen Zugriffen im Netzwerk und kann somit Angriffe auf Infrastrukturen rechtzeitig identifizieren. Ausführliche Bedrohungsdaten ermöglichen zudem eine zeitnahe Reaktion, um möglichst Schäden und den Verlust vertraulicher Daten zu vermeiden und damit die Business Continuity sicherzustellen.

Weitere Informationen finden Sie unter:
www.trendmicro.de/deep-discovery

Einen ausführlichen Testbericht erhalten Sie unter:
www.trendmicro.de/unternehmen/cyber-sicherheit/nss-labs-report/