Das IT-Sicherheitsgesetz 2015

AKTUELLES:

Schon 2010, seit der Entdeckung und Veröffentlichung von Stuxnet, einem Wurm, der die Motorsteuerung diverser kritischer Systeme wie Wasserwerke und Kernkraftwerke ermöglichte, müssen sich Betreiber von IT-Landschaften nicht nur um die Sicherheit ihrer Daten sorgen, sondern auch um Bürger, die von dem Betrieb dieser IT-Umgebungen abhängig sind.
Jüngste Beispiele, wie der 2015 erfolgte Cyber-Angriff auf den Deutschen Bundestag oder die erfolgreiche Ransomware-Infizierung des Lukaskrankenhauses aus dem Februar 2016 zeigen, dass Deutschland ein attraktives Angriffsziel ist. Auch in Zukunft werden Advanced Persistant Threats (APT), aber auch weiterentwickelte Malware eine Gefahr nicht nur für Daten, sondern auch für Menschen darstellen.

DER LOGISCHE SCHRITT:

Um diesen und weiteren Angriffen auch in Zukunft besser entgegenwirken zu können, wurde das neue, am 25. Juli 2015 in Kraft getretene IT-Sicherheitsgesetz verabschiedet. Vorhandene Gesetze, wie das Gesetz vom Bundesamt für Sicherheit in der Informationstechnik (BSIG) oder das Telemediengesetz (TMG), wurden geändert, um die Verbesserungen branchenspezifischer Mindeststandards sicherzustellen. Diese ermöglichen es, wichtige Verbesserungen der IT-Sicherheit in Deutschland zu realisieren. Auch wenn diese branchenspezifischen Sicherheitsstandards noch nicht finalisiert und deren Eignung durch das BSI festgestellt worden sind, so können doch schon heute Unternehmen an Hand der BSI IT-Grundschutz-Kataloge beleuchtet werden. Diese IT-Grundschutz-Kataloge stellen einen De-Facto-Standard für IT-Sicherheit dar und orientieren sich an den Vorgaben der Zertifizierung nach ISO 27001, die auf der Basis von IT-Grundschutz beim BSI beantragt werden kann. Weitere Informationen dazu gibt es auf der Homepage des BSI (https://www.bsi.bund.de).

WER BETROFFEN IST:

Die kürzlichen Gesetzesänderungen gelten vor allem für KRITIS-Betreiber, d.h. Unternehmen, die kritische Infrastrukturen betreiben. Ausfälle der IT-Systeme einer kritischen Infrastruktur können ernsthafte Versorgungsengpässe, starke Auswirkungen auf die öffentliche Sicherheit oder andere schwerwiegende Folgen für das Allgemeinwohl nach sich ziehen. Folgende Bereiche werden durch das IT-Sicherheitsgesetz als Sektoren definiert, denen kritische Infrastrukturen angehören:

KRITIS

- Energie
- Informationstechnik und Telekommunikation (Sprach- und Datenübertragung, Speicherung und Verarbeitung von Daten)
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheit (Pharma, Krankenhäuser, Medizinische Versorgung, …)
- Wasser (Trinkwasserversorgung, Abwasserbeseitigung)
- Ernährung

WAS ZU TUN IST:

KRITIS-Unternehmen sind nach einer Übergangsfrist von zwei Jahren ab Inkrafttreten einer Rechtsverordnung zur Bestimmung kritischer Infrastrukturen verpflichtet, branchenspezifische Mindestanforderungen an die IT-Sicherheit zu erfüllen. Noch offen ist die Entwicklung von branchenspezifischen, durch das BSI anerkannten Mindeststandards. Diese sollen später als Erfüllungsgrad und Überprüfungslinie des BSI dienen, um die angewendeten Anforderungen zu messen.

Die Maßnahmen zur Erfüllung des Mindeststandards müssen „angemessen“ sein und orientieren sich am „Stand der Technik“. Angemessen heißt, dass der erforderliche Aufwand zur Absicherung der kritischen Infrastrukturen im richtigen Verhältnis zu den Folgen eines Ausfalls oder deren Beeinträchtigung stehen muss. Mit „Stand der Technik“ wird verdeutlicht, dass technische Entwicklungen schneller als Gesetzgebungen erfolgen und daher keine konkreten technischen Anforderungen in Gesetzen genannt werden. „Stand der Technik“ ist ein gängiger juristischer Begriff.

Ebenfalls obliegt es den KRITIS-Betreibern, die Maßnahmen und deren Durchführung ausreichend zu dokumentieren und in Sicherheits- und Notfallkonzepten zu integrieren sowie gegenüber dem BSI die Erfüllung der Anforderungen alle zwei Jahre nachzuweisen.

Mit Inkrafttreten einer noch zu erlassenden Rechtsverordnung zur Bestimmung kritischer Infrastrukturen beginnt eine 2-jährige Übergangsphase, in der die branchenspezifischen Mindestanforderungen an die IT-Sicherheit umgesetzt werden müssen. Die Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen liegt in einer Entwurfsfassung vom 13. Januar 2016 vor, so dass mit deren baldiger Verabschiedung zu rechnen ist.

Weiterhin sind die KRITIS-Unternehmen verpflichtet, dem BSI eine Kontaktstelle zu benennen, die für die Kommunikation mit dem BSI über Sicherheitsangelegenheiten zuständig und verantwortlich ist.

Über die Kontaktstelle müssen KRITIS-Betreiber Sicherheitsrisiken an den BSI melden, so dass weitere KRITIS-Unternehmen zeitnah über Bedrohungen informiert werden können. Die Informationen werden zunächst anonymisiert weitergegeben. Sollte der gemeldete Ausfall oder die Beeinträchtigung jedoch schwere Folgen für Bund und Bundesbürger nach sich ziehen, können KRITIS-Unternehmensinformationen durchaus auch mit publiziert werden.

Verstöße gegen das IT-Sicherheitsgesetz können mit Geldbußen von bis zu 100.000 € sanktioniert werden.

WAS UNTERNEHMEN JETZT SCHON TUN KÖNNEN:

Bereits jetzt können sich KRITIS-Unternehmen an vorhandenen Empfehlungen des BSI IT-Grundschutz-Katalogs, oder an etablierten Standards, wie der Entwicklung eines gültigen Informationssicherheits-Managementsystems (ISIM) aus dem ISO 27001, orientieren. In vielen Punkten wird sich das BSI auch weiterhin an vorhandenen und bereits umgesetzten IT-Standards orientieren.

WIE TREND MICRO DEEP SECURITY SCHON JETZT HELFEN KANN:

Trend Micro Deep Security erstellt kostenoptimierend und effizient IT Security Reports und unterstützt bei der Erfüllung von diversen Compliance-Anforderungen.

DAS „SECURITY-TASCHENMESSER“

Trend Micro Deep Security zeichnet sich durch seine Flexibilität und ein umfangreiches Feature-Set aus. Ob physikalisch, virtuell oder cloudbasierte Clients und Server, Deep Security sichert Systeme schnell, einfach und automatisiert ab. Der modulare Aufbau von Deep Security erlaubt es, aus Antimalware, Web Reputation, Host Firewall, Intrusion Prevention, Integrity Monitoring und Log Inspection auszuwählen und diverse Dienste, wie File-, Web-, Datenbankserver, zu schützen.

DIE DEEP SECURITY MODULE IM ÜBERBLICK:

Antimalware: Kombiniert mit Trend Micro Smart Protection Network bietet das Antimalware-Modul schnellen und umfangreichen Schutz für bekannte Schadsoftware.

Web Reputation: Mit Web Reputation und dem sich stets weiterentwickelnden Smart Protection Network werden schädliche und nicht vertrauenswürdige Internet-Quellen geblockt, um das System vor schädlichen Kommunikationen mit dem Internet zu schützen.

Host Firewall: Die umfangreiche Host Firewall erlaubt die volle Kontrolle über den Netzwerkverkehr des Systems.

Intrusion Prevention: Zusammen mit einem umfangreichen Exploit-Katalog und dem Recommendation Scan ermöglicht das Intrusion Prevention Modul schnell und gezielt Sicherheitslücken auf dem System zu schließen, ohne das System zu beeinträchtigen oder es neu zu starten.

Integrity Monitoring: Die Integrität von System- als auch persönlichen Daten ist unerlässlich für die Erfüllung von Richtlinien und vollständiger Sicherheit. Das Integrity Modul erlaubt, bekannte Systeme und selbst definierte Daten zu überwachen und somit zu schützen.

Log Inspection: Das Log Inspection-Modul lässt bekannte Logdaten des Systems nach definierten Kriterien überwachen, um so auf bestimmte Ereignisse in der Systemlandschaft schneller zu reagieren.

Die nahtlose Integration in die Systemlandschaft, sowie die Nutzung von Virtual Patching für Sicherheitslücken ohne Eingriff ins System oder Reboots, ermöglichen es, schnell auf Angriffe zu reagieren. Somit zeichnet sich Deep Security als wahres Security-Taschenmesser aus, das in keinem Security Portfolio der Infrastruktur fehlen sollte.

DEEP SECURITY REPORTS

Der Deep Security Manager gibt einen schnellen Einblick in die aktuelle Infrastruktur. Ob physisch, virtuell oder cloudbasiert, sämtliche Sicherheitsstände der Server und Clients sind auf einen Blick sichtbar. Konfigurierbare Reports ermöglichen es, Audit Reports nach Vorgaben der Audit-Richtlinien bereitzustellen. Mithilfe des Deep Security Managers lassen sich zeitnahe Reports zur Verfügung stellen – entsprechend der Meldepflicht des IT Sicherheitsgesetzes.

REPORTS - ANBINDUNG AN 3RD PARTY SOLUTIONS

Um die Reaktionszeit auf Angriffe noch zu verringern, bietet Deep Security die Möglichkeit, Events an SIEM Systeme, wie HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic und andere Systeme bereitzustellen. Auch die integrierte Deep Security API erlaubt es, Deep Security mit der bestehenden Reportinginstanz zu verbinden.

COMPLIANCE-ERFAHRUNG

Der BSI IT-Grundschutzkatalog orientiert sich an den bestehenden ISO 27001 Compliance-Anforderungen. Mit Deep Security erreicht man nicht nur einen hochqualitativen Sicherheitsstandard in der Infrastruktur und Abdeckungen diverser Anforderungen aus ISO 27001. Deep Security ist auch ein Werkzeug, das die Erfüllung der Compliance diverser Regularien wie PCI DSS 3.0, HIPAA, HITECH, NIST oder SAS 70 unterstützt. Deep Security trägt damit nicht nur zum Bestehen wiederkehrender Audits bei, sondern ermöglicht Verantwortlichen kontinuierlich, den Compliance-Erfüllungsgrad zu verifizieren und aufrecht zu erhalten.

Über Trend Micro

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als fünfundzwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein internationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/

http://blog.trendmicro.de/

http://www.twitter.com/TrendMicroDE

TREND MICRO™

Securing Your Journey to the Cloud

TREND MICRO Deutschland GmbH
Zeppelinstrasse 1
85399 Hallbergmoos
Deutschland
Tel. +49 (0) 811 88990-700
Fax +49 (0) 811 88990-799

TREND MICRO Schweiz GmbH
Schaffhauserstrasse 104
8152 Glattbrugg
Schweiz
Tel. +41 (0) 44 82860-80
Fax +41 (0) 44 82860-81

TREND MICRO (SUISSE) SÀRL
World Trade Center
Avenue Gratta-Paille 2
1018 Lausanne
Schweiz

www.trendmicro.com