esatus AG
Enforcing Information Security

IT-Sicherheitsgesetz und EU-Datenschutzgrundverordnung

Effiziente Projektierung zur Erfüllung neuer Anforderungen an den Stand der Technik.
Veröffentlicht am 16.10.2017 auf www.digitaleweltmagazin.de

Steigende regulatorische Anforderungen

Die letzten Jahre waren geprägt von verschiedenen neuen Gesetzgebungen, insbesondere im Bereich des Datenschutzes und der IT-Sicherheit. Die Anforderungen, die aktuell am stärksten in Ihrer Umsetzung in Deutschland diskutiert werden, sind das IT-Sicherheitsgesetz (ITSiG) und die EU-Datenschutzgrundverordnung (EU-DSGVO). Insbesondere die EU-DSGVO, welche am 25.05.2018 den Datenschutz in der gesamten EU neu aufstellen wird, schafft Anforderungen an Prozesse und Sicherungsmaßnahmen für Technologien, die personenbezogene Daten verarbeiten. Werden die neuen Anforderungen nicht erfüllt, so werden Sanktionen in Höhe von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes des Unternehmens fällig, je nachdem welcher Betrag höher ist. Das Thema des technischen Datenschutzes (Data Privacy by Design and by Default) war nie relevanter. Im BDSG (Bundesdatenschutzgesetz) waren Regelungen zur Absicherung von Technologien durch technische und organisatorische Maßnahmen (TOM) noch als „soft law" definiert, also ohne konkrete Sanktionierung bei Nicht-Erfüllung. Dies ändert sich durch die EU-DSGVO, da nun bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes fällig werden

können, wenn Richtlinien des technischen Datenschutzes nicht umgesetzt sind. Darüber hinaus stellt das IT-Sicherheitsgesetz neue Anforderungen an die IT-Sicherheit für Betreiber kritischer Infrastrukturen und Betreiber von Telemedien. Beide Gesetzgebungen haben einen wesentlichen Faktor gemeinsam: Den Stand der Technik. Der Stand der Technik ist ein bewusst offen definierter Rechtsbegriff. Nach ITSiG und EU-DSGVO sollen IT-Sicherheitsmaßnahmen und der technische Datenschutz in ihren technischen und organisatorischen Maßnahmen den aktuellen Stand der Technik nachweisen. Im Gesetz selbst (EU-DSGVO) ist als Methode gemäß Stand der Technik lediglich die Pseudonymisierung genannt, durch die Datensätze bspw. durch Verschlüsselungen so verändert werden, dass sie keine Identifizierbarkeitsfaktoren für die jeweilige Person beinhalten. Da der Rechtsbegriff sehr offen definiert ist, haben viele Unternehmen keinen klaren Durchblick, was dieser Stand der Technik nun für einen selbst bedeutet. Eine erste Einordnung, was der aktuelle Stand der Technik ist, gibt die Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes vom TeleTrusT – Bundesverband IT-Sicherheit e. V. aus dem Jahre 2016. Hier werden Anforderungen an sichere Vernetzung, sichere Internetverbindungen, Digital Enterprise Security, Client- und Serversicherheit, Mobile Security sowie gängige Standards und Normen zur Nachweisung des Stands der Technik von IT-Sicherheitsexperten und Juristen beleuchtet.

Unternehmen, die nicht schon durch das bereits eingetretene ITSiG den Stand der Technik erfüllen müssen, sollten sich priorisiert mit Bestandsanalysen der Sicherungsmaßnahmen von Technologien beschäftigen, die personenbezogene Daten verarbeitet, um zum Stichtag des 25.05.2018 konform zu den neuen Anforderungen der EU-DSGVO zu sein. Für diese Herausforderung ist ein Projektteam aus IT-Sicherheitsexperten und Juristen notwendig, um die juristischen Anforderungen mit wirkungsvollen Methoden der IT-Sicherheit zu kombinieren. Betreiber kritischer Infrastrukturen oder Anbieter von Telemedien, die sich mit noch keiner der beiden neuen Gesetzgebungen beschäftigt haben, sollten eine Kombination beider Problemstellungen anstreben. Im Unternehmensberatungskontext fällt oft auf, dass gerade größere Unternehmen oftmals Projektieren ohne eine Abstimmung mit anderen Fachabteilungen voranzustellen. Als Konsequenz werden die gleichen Problemstellungen individuell von den jeweiligen Fachabteilungen behandelt, mehrere Software-Tools implementiert, welche die gleichen Problemstellungen lösen sollen und Synergieeffekte verschiedener Herausforderungen völlig ausgeblendet. Dies ist ineffizient und erzeugt unnötige Kosten in mehrstelliger Millionenhöhe. Eine effiziente Kombination beider Herausforderungen für Betreiber kritischer Infrastrukturen oder Betreiber von Telemedien könnte wie folgt aussehen:

1. Schnittmengen und GAP-Analyse

Im ersten Schritt sollten Unternehmen Technologien, Prozesse und IT-Infrastrukturkomponenten identifizieren, die sowohl unter den Schutzbedarf des technischen Datenschutzes nach EU-DSGVO fallen, als auch vom ITSiG betroffen sind. Sind diese identifiziert, sollte im Zuge einer GAP-Analyse die Kluft zwischen IST-Zustand und SOLL-Zustand der neuen regulatorischen Anforderungen erörtert werden. Aus dieser Analyse lassen sich Maßnahmen ableiten, die umgesetzt werden müssen, um in Zukunft gesetzeskonform agieren zu können. Eine Betrachtung der Technologien, Prozesse und IT-Infrastrukturkomponenten sollte dabei nicht nur durch Juristen erfolgen, sondern auch durch IT-Sicherheitsspezialisten, die mit „Bits und Bytes“ umgehen können. Die identifizierten GAPs zu beiden neuen regulatorischen Anforderungen sollten priorisiert behandelt werden, da diese mit den höchsten Risiken für Unternehmen einhergehen, wenn die regulatorischen Anforderungen nicht beachtet werden.

2. Technische Nachbesserung

Die identifizierten GAPs aus Schritt 1 sollten im nächsten Schritt eliminiert werden. GAPs mit hohem IT-Impact benötigen eine höhere Vorlaufzeit zur Beseitigung als solche, die reine Dokumentationen voraussetzen. Die Erstellung eines Zeitplans unter

Berücksichtigung des IT-Impacts scheint also der effizienteste Weg, um technische Nachbesserungen bis zum Stichtag des 25.05.2018 bewältigen zu können. Wer noch nicht gestartet hat, sollte dies schleunigst tun.

3. Dokumentationen

Sind die technischen Nachbesserungen abgeschlossen, sollten alle fehlenden Dokumentationen erstellt werden und bestehende Dokumentationen nachgebessert bzw. erweitert werden. Im Zuge der Dokumentationserstellung sollte man sich an den Richtlinien der ISO 27001 orientieren. Dadurch ebnet man den Weg zu einer ISO 27001 Zertifizierung, die mit hoher Wahrscheinlichkeit in Zukunft der Maßstab zur Vorweisung der Erfüllung des Stands der Technik werden kann.

4. Kontinuierliches Information Security Management System (ISMS)

Sind technische und dokumentarische Anforderungen bis zum Stichtag umgesetzt, ist das „Projekt" IT-Sicherheit noch lange nicht abgeschlossen. Angriffsvektoren nehmen von Jahr zu Jahr zu, bewährte Verschlüsselungsverfahren könnten durch steigende Rechenleistung leicht zu entschlüsseln werden und der Stand der Technik ist morgen schon nicht mehr der, welcher er heute ist. Die Implementierung eines kontinuierlichen Information Security Management Systems ist nicht nur Voraussetzung zur Erlangung einer ISO 27001 Zertifizierung. Wenn Unternehmen IT-Sicherheit und Datenschutz wirklich ernst nehmen und ihre Daten umfassend schützen möchten, sollten sie in regelmäßigen Abstände den Stand der Technik in technischen und organisatorischen Maßnahmen zur Absicherung gegen Cyberangriffe und Datenverluste überprüfen.

Eine gemeinsame Betrachtung des ITSiG und der EU-DSGVO im Sinne des Stands der Technik ist kosteneffizient und führt zu einer klaren Definition der IT-Faktoren im Unternehmen, die sich im Falle eines Angriffs am negativsten auf das Unternehmen auswirken könnten. Leider ist der dargestellte Weg der Projektierung in vielen Unternehmen reines Wunschdenken, da Fachabteilungen zu unabhängig voneinander agieren und meist die generelle Aufmerksamkeit für die Thematik nicht vorhanden ist. Zu sehr werden regulatorische Anforderungen, insbesondere im Datenschutz, als notwendige Übel wahrgenommen, welche so lange ignoriert werden, bis Audit-Findings Unternehmen zur Handlung zwingen. Das bis zu diesem Zeitpunkt bereits Gigabytes an kritischen Daten durch Cyberangriffe in falsche Hände geraten können, scheint oftmals nicht in der Aufmerksamkeit zu stehen. Dies bestätigen zuletzt die gezielten Angriffe auf Größen der Unternehmensberatungsbranche. Daher ist zu empfehlen: Projektieren Sie frühzeitig, stärken Sie Ihre Aufmerksamkeit zu Fragestellungen der IT-Compliance und erschließen Sie Synergiepotentiale!

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Getreu der Unternehmensmission „Enforcing Information Security" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln des Unternehmens richtet.

Herausgeber **esatus** AG

Grafik Seite 1 © Fotolia / jijomathai

Weitere Informationen zum Thema „IT-Sicherheitsgesetz und Datenschutzgrundverordnung" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: Oktober 2017