www.pwc.de/LogistikKompass

Transport & Logistik Kompass

November 2017

Das IT-Sicherheits-gesetz verpflichtet

Das neue IT-Sicherheits-gesetz fordert von den Betreibern kritischer Infra-strukturen die Einrichtung eines auditierten Informationssicherheits-managementsystems. Wir geben Ihnen einen ersten Überblick über die Anforderungen.

pwc

Das IT-Sicherheitsgesetz verpflichtet

Der Hintergrund

Traditionelle Versorgungsnetzwerke in den Bereichen Strom, Telekommunikation oder Transport werden fast ausschließlich digital gesteuert. Dabei verknüpfen sich bislang getrennte Unternehmens oder Prozessnetzwerke immer stärker mit dem Internet.

Die wachsende Vernetzung bietet große Chancen für die beteiligten Unternehmen. Zugleich stellt sie aber auch eine wachsende Angriffsfläche für Cyberattacken dar – mit zum Teil weitreichenden Konsequenzen. Zum Schutz der Telekommunikations- und elektronischen Datenverarbeitungssysteme von Betreibern kritischer Infrastrukturen hat das Bundesministerium des Innern (BMI) gemeinsam mit deutschen Infrastruktur-Unternehmen und deren Interessenverbänden den Umsetzungsplan zum Schutz kritischer Infrastrukturen (kurz „UP KRITIS“) erarbeitet. Das daraus abgeleitete und seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) soll mit seinen Rechtsverordnungen den IT-Standort Deutschland langfristig sichern.

Seit dem 30. Juni 2017 tickt die Uhr für Betreiber kritischer Infrastruktur

Transport- und Verkehrsunternehmen mit kritischer Infrastruktur müssen zum Schutz ihrer digitalen Nervenstränge zukünftig ein Informationssicherheits-Management-System (ISMS) einführen.

Am 29. Juni 2017 wurde die „Erste Verordnung zur Änderung der BSI-Kritisverordnung“ im Bundesgesetzblatt veröffentlicht. Sie konkretisiert das IT-Sicherheitsgesetz und legt unter anderem die Kriterien zur Bestimmung kritischer Infrastrukturen im „Sektor Transport und Verkehr“ fest. Mit dem Datum der Veröffentlichung greifen auch die im IT-Sicherheitsgesetz genannten Fristen für diejenigen Unternehmen im Transport- und Verkehrswesen, die mindestens einen der in der Rechtsverordnung genannten Schwellwerte überschreiten.

1 Betroffene Unternehmen haben nun enge Fristen einzuhalten

Bei der Festlegung der Kriterien folgte der Gesetzgeber in weiten Teilen den Größenordnungen, die im zuletzt veröffentlichten Referentenentwurf der Rechtsverordnung benannt wurden. Dieser wurde durch eine Fokussierung der Kriterien auf die kritischen Bereiche im Vergleich zu den früheren Entwürfen stark verändert.

Die Anzahl von Unternehmen, die unter die Regelung des Gesetzes fallen, ist überschaubar. Sie stammen aus den Bereichen Luft-, Schienen- und Straßenverkehr, der See- und Binnenschifffahrt, dem ÖPNV und der Logistik. Auch einige Spezialunternehmen des Sektors Transport und Verkehr zählen dazu.

So fallen zum Beispiel Anlagen oder Systeme zur Passagierabfertigung an Flughäfen darunter, die mindestens 20 Millionen Passagiere pro Jahr abfertigen. Auch Leitzentralen der Eisenbahnverkehrsunternehmen ab einer disponierten Güterverkehrs-Transportleistung von 730 Millionen Tonnen pro Jahr zählen zur kritischen Infrastruktur. Schienennetz und Stellwerke der Eisenbahn hingegen werden nur dann dazu gerechnet, wenn diese zum Kernnetz des transeuropäischen Verkehrsnetzes (Kernnetz nach TEN-V) zählen.

Folgende Kriterien hat der Gesetzgeber festgeschrieben:

Tab. 1 Kriterien zur Bestimmung kritischer Infrastruktur

Dienstleistung	Anlagenkategorie (Bemessungskriterium pro Jahr)	Schwellenwert
Personen- und Güterverkehr im Luftverkehr	Anlage oder System zur Passagierabfertigung an Flugplätzen (Anzahl der Passagiere/Jahr)	20.000.000
	Anlage oder System zur Frachtabfertigung an Flugplätzen (Gütermenge in Tonnen/Jahr)	750.000
	Infrastrukturbetrieb eines Flugplatzes (Gütermenge in Tonnen/Jahr)	750.000
	Infrastrukturbetrieb eines Flugplatzes (Anzahl der Passagiere/Jahr)	20.000.000
	Flugsicherung und Luftverkehrskontrolle (Anzahl Flugbewegungen/Jahr)	17.500
Schienenverkehr der Eisenbahn	Personenbahnhof der Eisenbahn (Bahnhofskategorie)	jeweils höchste Kategorie
	Güterbahnhof (Anzahl ausgehender Züge/Jahr)	23.000
	Zugbildungsbahnhof (Anzahl gebildete Züge/Jahr)	23.000
	Schienennetz und Stellwerke der Eisenbahn (Schienennetz nach TEN-V)	Kernnetz
	Verkehrssteuerungs- und Leitsystem der Eisenbahn (Leitsystem des Schienennetzes nach TEN-V)	Kernnetz
	Leitzentrale der Eisenbahn (disponierte Transportleistung • Personenverkehr in Zugkilometer/Jahr pro Netz/Teilnetz oder • Güterverkehr in Tonnenkilometer/Jahr)	 8.200.000 730.000.000
See- und Binnen-schifffahrt	Anlage oder System zum Betrieb von Bundeswasserstraßen (Güterverkehrsdichte in Tonnen)	17.000.000
	Verkehrssteuerungs- und Leitsystem der See- und Binnenschifffahrt (Güterverkehrsdichte in Tonnen)	17.000.000
	Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt (Disponierte Frachtmenge in Tonnen/Jahr)	1.875.000
	Anlage oder System zur Disposition von Binnenschiffen (nur Güterverkehr) (disponierte Transportleistung in Tonnenkilometer/Jahr)	345.000.000
Straßenverkehr	Verkehrssteuerungs- und Leitsystem (Verkehrssteuerungs- und Leitsystem der Bundesfernstraßen)	Verkehrssteuerungs- und Leitsystem für das Netz der Bundesautobahnen
	Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr (Anzahl Einwohner der versorgten Stadt)	500.000
ÖPNV	Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV) (Anzahl Fahrgäste/Jahr)	125.000.000
	Verkehrssteuerungs- und Leitsystem des ÖPNV (Anzahl Fahrgäste/Jahr)	125.000.000
	Leitzentrale des ÖSPV (Betreiber, Verkehrsunternehmen) (Anzahl Fahrgäste/Jahr)	125.000.000
Logistik	Anlage oder System zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik (Gütermenge in Tonnen/Jahr)	17.000.000
	Anlage oder IT-System zur Logistiksteuerung- oder Verwaltung in den Segmenten Massengut, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik (Gesamtmenge bereitgestellte, verteilte, gelagerte, bearbeitete oder umgeschlagene Gütermenge in Tonnen/Jahr)	17.000.000
Sonstige	Anlage zur Wettervorhersage, zur Gezeitenvorhersage oder zur Wasserstandsmeldung (Gesetzliche Verpflichtung zur Diensterbringung)	Anlagen im Sinne des §4 Absatz 1 DWD-Gesetz oder des §1 Absatz 9 SeeAufgG
	Satellitennavigationssystem (Betrieb der Bodeninfrastruktur)	Anlagen im Sinne des Artikels 28 der Verordnung (EU) Nr. 1285/2013

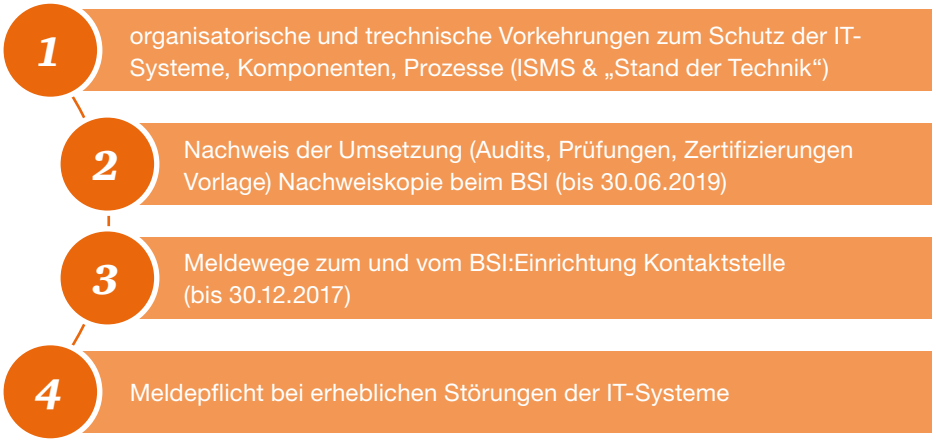
Der Zeitraum für die Bemessung reicht vom 1. April bis zum 31. März des Folgejahres. Ob die Kriterien erfüllt wurden, muss der Betreiber jeweils zum 31. März eines Jahres für das zurückliegende Jahr ermitteln.

Der Gesetzgeber verwendet den Begriff Anlagen, der für die Berechnung der Schwellenwerte sehr wichtig ist. Stehen mehrere Anlagen in einem engen räumlichen sowie betrieblichen Zusammenhang – und erreichen oder überschreiten diese die Schwellenwerte zusammen, gilt die gesamte Anlage als kritische Infrastruktur. Der Gesetzgeber sieht diesen Zusammenhang bereits als gegeben, wenn die Anlagen:

- auf demselben Betriebsgelände liegen,
- mit gemeinsamen Betriebseinrichtungen verbunden sind,
- einem vergleichbaren technischen Zweck dienen und
- unter gemeinsamer Leitung stehen.

In der Interpretation des IT-Sicherheitsgesetzes ist eine betroffene Einrichtung – neben einer Vielzahl weiterer Maßnahmen – verpflichtet, **bis zum 30. Dezember 2017** eine „Kontaktstelle für die Kommunikationsstrukturen" gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu benennen. Dabei müssen die Betreiber sicherstellen, dass sie jederzeit erreichbar sind. Zudem sind sie **bis zum 30. Juni 2019** verpflichtet, ein ISMS einzurichten, die technischen und organisatorischen Maßnahmen am „Stand der Technik"1 auszurichten und die Erfüllung dieser Anforderungen gegenüber dem BSI nachzuweisen.

Abb. 1 Kernforderungen an Betreiber kritischer Infrastrukturen



Das Gesetz regelt darüber hinaus, dass die nicht sachgerechte Umsetzung von Maßnahmen als Ordnungswidrigkeit behandelt wird und je Einzelfall mit einer Geldbuße von bis zu 100.000 Euro geahndet werden kann. Ordnungswidrig handelt demnach zu m Beispiel, „wer vorsätzlich oder fahrlässig […] entgegen §8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach §10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht vollständig oder nicht rechtzeitig trifft"2.

Ferner ist das BSI gegenüber dem Betreiber kritischer Infrastrukturen sanktionsberechtigt und kann fristbewehrte Auflagen erteilen.

Unabhängig von den gesetzlichen Regelungen ist jedes Unternehmen der Branche gut beraten, sich mit dem Thema Cybersicherheit im Rahmen einer ganzheitlichen Betrachtung des Risiko- und Notfallmanagements über die IT hinaus ganz grundsätzlich auseinanderzusetzen.

[1] Der „Stand der Technik" ist ein unbestimmter Rechtsbegriff, der sich allerdings in der gängigen Rechtsauffassung als „über die anerkannten Regeln der Technik hinausgehend" gefestigt hat. Er erfordert umfassende Maßnahmen, die technisch möglich und nicht nur nötig sind.
[2] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, Art. 1, §14, Abs. 1, Satz 1.

2 Die Vorgaben sind für viele Betreiber eine große Herausforderung

Die organisatorischen und technischen Vorkehrungen zum Schutz der IT-Systeme, sowie Komponenten und Prozesse zu schaffen, bedeutet für viele Betreiber kritischer Infrastrukturen ein Projekt mit einer Laufzeit von im besten Fall einem Jahr. In der Praxis ist meist von einem längeren Zeitraum auszugehen. Angesichts der bereits laufenden Fristen besteht für Unternehmen, die noch nicht aktiv geworden sind, akuter Handlungsbedarf.

Nach unserer Erfahrung sind mehrere Erfolgsfaktoren für das Projekt ausschlaggebend:

- Die Geschäftsleitung begreift das Projekt als gesamtheitliche Sicherheitsaufgabe, die nicht allein auf die IT reduziert und nicht an diese delegiert werden darf. Insofern sollte ein Mitglied der Geschäftsleitung als Projektsponsor auftreten.
- Die Geschäftsleitung sollte mit Zustimmung der Mitbestimmungsgremien einen Informationssicherheitsbeauftragten bestellen, der direkt an die Geschäftsführung berichtet und im Interesse zügiger Entscheidungen die volle Rückendeckung genießt.
- Selbst unter Einbeziehung externer Unterstützung stehen mindestens zwei Mitarbeiter, je einer für technische und organisatorische Projektaufgaben, für das Projekt zur Verfügung. Sie sind für die Projektdauer von anderen regulären Tätigkeiten weitgehend zu entlasten.
- Die Iterationszyklen bei der Etablierung von Rollen und Verantwortlichkeiten, der Einführung von Sicherheits-Leitlinien und anderen Regelungsdokumenten zur Informationssicherheit, bei der Risikobestimmung und allen anderen projektimmanenten Abstimmungsverfahren umfassen zwei, maximal drei Durchläufe.
- Wenn Dritte Teile der kritischen Infrastruktur betreiben, sind diese frühzeitig in die Planung einzubeziehen. Deren Funktion muss eng mit dem ISMS des Unternehmens verzahnt werden.

Als besonders schwierig erweist sich jedoch in der Praxis häufig die technische Absicherung älterer Prozess-IT, die sich nicht so einfach durch neue Systeme ablösen lässt.
Externe Zugänge zur Wartung, proprietäre oder potenziell unsichere Betriebssysteme können auf der einen Seite eine erhebliche Gefahr für die Sicherheit aller übri gen IT-Systeme darstellen. Auf der anderen Seite können solche Systeme ihrerseits durch Schadsoftware aus anderen Bereichen in ihrer Funktionsfähigkeit beeinträchtigt werden. Prominente Beispiele für nachhaltige Störungen waren die Ransomware-Zwischenfälle in der jüngeren Vergangenheit in verschiedenen Unternehmen.

Wenn hier nicht bereits im Vorfeld die IT oder die abgrenzenden Systeme am „Stand der Technik“ ausgerichtet wurden, kommt auf die betroffenen Einrichtungen ein erheblicher Aufwand sowohl bei der Planung als auch bei der technischen Umsetzung der Sicherungsmaßnahmen zu.

Unser Angebot
Wir unterstützen Sie dabei, die Vorgaben des IT-Sicherheitsgesetzes umzusetzen. Wir kennen die Stolpersteine und Fallstricke auf dem Weg in die Praxis. PwC hat bereits mehrere Betreiber kritischer Infrastrukturen bei diesem Prozess über alle Projektphasen umfassend begleitet. Insbesondere bei Routinearbeiten können wir mit unseren umfangreichen Erfahrungen erhebliche Synergieeffekte schaffen.

Damit Unternehmen ihrer Nachweispflicht nachkommen können, übernehmen unsere akkreditierten Auditoren auch die Zertifizierung des ISMS.

Ihre Ansprechpartner

Ingo Bauer
Essen
Tel.: +49 201 438-1107
ingo.bauer@de.pwc.com

Derk Fischer
Düsseldorf
Tel.: +49 211 981-2192
derk.fischer@de.pwc.com

Hendrik Gollnisch
Berlin
Tel.: +49 30 2636-1500
hendrik.gollnisch@de.pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 158 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. Mehr als 10.600 engagierte Menschen an 21 Standorten. 2,09 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.