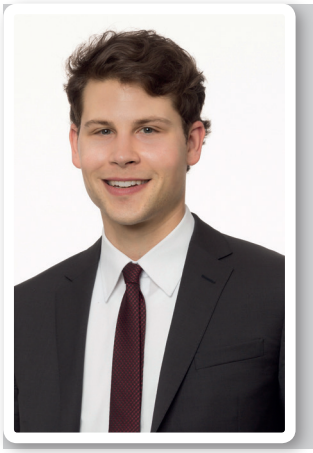
Die Umsetzung des NIS-Gesetzes

Das Netz- und Informationssystemsicherheitgesetz »NISG« ist am 29. Dezember 2018 heimlich, still und leise in Kraft getreten. Was bedeutet das nun konkret für »Betreiber wesentlicher Dienste«?



»Umsetzung des NISG nicht ausschließlich an die IT delegieren.«

Tobias Tretzmüller ist Rechtsanwalt in ständiger Kooperation mit Knyrim Trieb Rechtsanwälte. Er berät und vertritt Unternehmen in den Bereichen IT-Softwarevertragsrecht, Urheberrecht, Datenschutzrecht und in Behörden- und Zivilverfahren in diesen Materien (IT-Litigation). Er ist zertifizierter Datenschutzbeauftragter und TÜV-geprüfter ISO-27001-Auditor.

Haben Sie Lust auf ein Gedankenexperiment? Was würde geschehen, wenn die Stromversorgung dauerhaft zusammenbricht? Was hätte das für Konsequenzen für Ihren Alltag? Rasch würde wohl der Verkehr kollabieren. Danach würde die Situation in den Krankenhäusern eskalieren.

Was sich gut als Thriller liest, ist – wie Insider wissen – jeden Tag aufs Neue eine reale Gefahr. Das Ziel des NIS-Gesetzes ist es, derartige Katastrophenfälle zu verhindern. Nicht nur aufgrund dieser hehren Zielsetzung ist das NISG von Bedeutung.

>> Verpflichtungen für Betreiber wesentlicher Dienste <<

Bereits zwei Wochen nach Zustellung des Bescheids, mit welchem eine Qualifikation als Betreiber eines wesentlichen Dienstes erfolgt, müssen diese eine Kontaktstelle (»single point of contact«) für die Kommunikation mit dem Bundeskanzler, dem Bundesministerium für Inneres oder dem Computer-Notfallteam benennen. Diese Kontaktstelle muss jedenfalls in jenem Zeitraum erreichbar sein, in dem der Betreiber seinen Dienst zur Verfügung stellt – regelmäßig also rund um die Uhr.

Die wesentlichste präventive Verpflichtung ist, dass der Betreiber wesentlicher Dienste im Hinblick auf die Netz- und Informationssysteme geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen treffen muss. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein. Die Betreiber wesentlicher Dienste haben proaktiv alle drei Jahre nach Zustellung des oben genannten Bescheides die Erfüllung dieser Anforderungen nachzuweisen!

Erforderliches Schutzniveau: Das Ganze ist nur so stark wie sein schwächstes Glied.

Der Nachweis, dass adäquate Maßnahmen umgesetzt wurden, wird regelmäßig durch »Zertifizierungen« erfolgen. Praktisch wird dabei die ISO/IEC Norm 27001:2013 eine wichtige Rolle spielen.

Von dieser Verpflichtung können sich die Betreiber wesentlicher Dienste freilich nicht durch eine Auslagerung von kritischen Prozessen »befreien«. Die unmittelbaren Adressaten des NISG werden daher gut daran tun, ihre aus dem NISG erwachsenden Verpflichtungen auf ihre Erfüllungsgehilfen vertraglich zu überbinden. Nur wenn diese angemessen in das gesamte Sicherheitssystem integriert sind, wird es in Summe gelingen, das erforderliche Schutzniveau zu erreichen. Mit anderen Worten: Das NISG betrifft mittelbar sämtliche Dienstleister, die zu Betreibern wesentlicher Dienste Schnittstellen haben. Können diese das erforderliche Schutzniveau nicht gewährleisten, dann sind sie nicht geeignet, zur Netz- und Informationssicherheit beizutragen. Sicherheitsexperten wissen: Das Ganze ist nur so stark wie sein schwächstes Glied.

Weiters treffen Betreiber wesentlicher Dienste bei einem Sicherheitsvorfall Meldepflichten an das zuständige Computer-Notfallteam. Neben der Meldepflicht im Sinne des NISG werden parallel regelmäßig auch die Meldepflichten im Sinne der DSGVO zu beachten sein.

Der praktische Anwendungsbereich des NISG geht weit über die Betreiber wesentlicher Dienste hinaus. Es hat vielmehr Relevanz für sämtliche Unternehmen, die eine Schnittstelle zu einem unmittelbaren Adressaten des NISG haben. Lieferantenbeziehungen werden im Zuge der ISO-27001-Zertifizierung genau geprüft. Die Durchführung von Audits vor Ort sollte also nicht nur am Papier geregelt sein, sondern auch tatsächlich ausgeübt werden.

>> Ausblick und Empfehlung <<

Auch aufgrund des NISG ist damit zu rechnen, dass IT- und datenschutzspezifische Zertifizierungen zunehmen werden. Keinesfalls sollte die Umsetzung des Netz- und Informationssystemsicherheitgesetzes ausschließlich an die IT-Abteilung delegiert werden. Vielmehr ist eine projektspezifische Zusammenarbeit der Abteilungen Compliance, Recht, Risikomanagement, Datenschutz und IT gefragt, welche durch ein starkes Commitment der Unternehmensspitze getragen wird. Schließlich steht einiges auf dem Spiel. ■

Foto: beigestellt