„Eingeschränkt“ bis „streng geheim“

Mit Sicherheit mehr Information: Eine neue ÖNORM regelt den Zugang von Unternehmen zu klassifizierten Informationen.

Aufgrund von völkerrechtlichen Verpflichtungen oder innerstaatlichen Interessen können Informationen über bestimmte Tatsachen bei amtlichen Stellen geheimhaltungsbedürftig sein. Solche Informationen sind mit einer der Klassifizierungsstufen „Eingeschränkt“, „Vertraulich“, „Geheim“ oder „Streng geheim“ zu versehen.

Daraus ergeben sich Maßnahmen, die den Missbrauch der Information oder die Preisgabe an Unbefugte verhindern sollen. Wollen Unternehmen Zugang zu derart klassifizierten Informationen haben, brauchen sie unter anderem eine Sicherheitsunbedenklichkeitsbescheinigung von einer staatlichen Stelle, die bestätigt, dass sie den gesetzlich vorgesehenen Schutz für die jeweilige Klassifizierungsstufe sicherstellen können. Die Voraussetzungen, die Unternehmen dafür erfüllen müssen, werden nun durch die ÖNORM S2450 definiert und präzisiert. Damit ist klarer ersichtlich, an welche Bedingungen die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung geknüpft wird.

Einheitliche Schutzstandards. Die rechtlichen Rahmenbedingungen für den Umgang mit klassifizierten Informationen werden vor allem durch das Informationssicherheitsgesetz und die Informationssicherheitsverordnung vorgegeben. Sie regeln die Voraussetzungen und Schutzstandards, unter denen Bundesbedienstete und sonstige Personen oder Unternehmen Zugang zu klassifizierten Informationen erhalten können, wenn sie diese für dienstliche Aufgaben oder für die Ausübung von Tätigkeiten im öffentlichen Interesse benötigen. Das Informationssicherheitsgesetz wurde überwiegend aufgrund von völkerrechtlichen Verpflichtungen erlassen. Der Rat der EU fasste 2001 einen Beschluss über Sicherheitsvorschriften, wonach die Mitgliedstaaten geeignete Maßnahmen zu treffen hatten, um dafür zu sorgen, dass beim Umgang mit EU-Verschlusssachen innerhalb ihrer Dienste und Gebäude die Sicherheitsvorschriften des Rates eingehalten werden. Unter bestimmten Voraussetzungen können auch andere natürliche und juristische Personen Zugang zu klassifizierten Informationen erhalten. Interesse daran besteht vor allem im Forschungs- und Wirtschaftsbereich. Voraussetzung ist die beabsichtigte Teilnahme an einem konkreten klassifizierten Forschungsprojekt oder an einer konkreten klassifizierten Ausschreibung. Um auch außerhalb der Bundesverwaltung denselben Schutz sicherzustellen, wie vom Informationssicherheitsgesetz gefordert wird, ist die Einhaltung mehrerer Maßnahmenpakete bei Unternehmen erforderlich, die für die Ausstellung der Sicherheitsunbedenklichkeitsbescheinigung auch zu überprüfen sind. Klassifizierte Informationen der Stufe „Streng geheim“ können im Allgemeinen nicht an die Wirtschaft weitergegeben werden und sind daher auch nicht Gegenstand der ÖNORM S2450.

Sicherheitsmaßnahmen, die etwa Unternehmen mit kritischer Infrastruktur wie Kraftwerke zu treffen haben, sind nun in deiner ÖNORM geregelt.

Maßnahmenpakete. Die Vorkehrungen, die Unternehmen zu treffen haben und die in der Norm nun detailliert geregelt sind, gliedern sich grob in

- Maßnahmen der Unternehmenssicherheit,
- Maßnahmen der materiellen Sicherheit,
- Maßnahmen der personellen Sicherheit,
- organisatorische Maßnahmen und
- Maßnahmen der IKT-Sicherheit.

Unternehmen sollten dazu einen Corporate-Security-Management-Prozess einführen, den sie mit bereits gebräuchlichen nationalen oder internationalen Standards wie der ÖNORM S2403, ISO 9001 oder ISO 27001 umsetzen können. Ab

INFORMATIONSSICHERHEIT

Klassifizierungsstufen

Klassifizierte Informationen sind zur Wahrung des von den übermittelnden Stellen vorgesehenen Schutzes einer der folgenden Klassifizierungsstufen zuzuordnen:

EINGESCHRÄNKT: Wenn die unbefugte Weitergabe der Informationen den in Art. 20 Abs. 3 B-VG genannten Interessen zuwiderlaufen würde.

VERTRAULICH: Wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist.

GEHEIM: Wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde.

STRENG GEHEIM: Wenn die Informationen geheim und überdies ihr Bekanntwerden eine schwere Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen wahrscheinlich machen würde.

FOTO: WERNER SABITZER

der Stufe „Vertraulich“ brauchen Unternehmen einen Sicherheitsbeauftragten, der für die Umsetzung von Sicherheitsmaßnahmen verantwortlich ist. Er ist für Schulungen und Unterweisungen der Mitarbeiter zuständig, für organisatorische und technische Maßnahmen und für die vorgegebenen Aufzeichnungen. Maßnahmen der personellen Sicherheit umfassen insbesondere Sicherheitsüberprüfungen und Verlässlichkeitsprüfungen.

Die Voraussetzungen dafür sind im Sicherheitspolizeigesetz bzw. im Militärbefugnisgesetz geregelt. Maßnahmen der materiellen Sicherheit betreffen im Besonderen bauliche Maßnahmen sowie Zutrittskontroll- und Überwachungssysteme. Dabei hat sich das „Zwiebelschalenprinzip“ bewährt, wonach ein Zugriff umso wahrscheinlicher verhindert werden kann, je mehr unterschiedliche Widerstände dagegen eingerichtet werden. Der Sicherheitsbeauftragte trifft die Auswahl der Maßnahmen für den materiellen Geheimschutz auf Grundlage einer Einschätzung der Bedrohungslage, wobei ein Risikomanagementprozess anzuwenden ist, der einem gängigen Standard folgen kann. Physische Schutzmaßnahmen von besonders zu schützenden Bereichen in Unternehmen müssen mehrere technische Standards für Widerstandsklassen berücksichtigen.

Zu den organisatorischen Maßnahmen zählt die Verpflichtung, klassifizierte Informationen eindeutig und gut erkennbar zu kennzeichnen. Ab der Stufe „Vertraulich“ ist auch deren Verwendung zu dokumentieren. Weitere Regeln betreffen die gesicherte Aufbewahrung, die Vervielfältigung und die Vernichtung von Informationen. Das Unternehmen muss einen Notfallplan aufstellen, der die Vorgangsweise bei außergewöhnlichen Situationen regelt. Darin ist unter anderem zu regeln, wie in Notsituationen vorgegangen wird, damit der unbefugte Zugang, die unbefugte Weitergabe oder der Verlust der Integrität bzw. der Verfügbarkeit der Information verhindert wird. Mit Maßnahmen der IKT-Sicherheit hat der Sicherheitsbeauftragte dafür Sorge zu tragen, dass auch die Verarbeitung von klassifizierten Informationen in Informations- und Kommunikationssystemen des Unternehmens durch besondere Sicherungsmaßnahmen wie z. B. Verschlüsselung geschützt ist. Der Umfang dieser Maßnahmen ist von der Klassifizierungsstufe abhängig.

Von Experten entwickelt. Durch das steigende Interesse von Unternehmen an Projekten im Bereich der Sicherheitsforschung hat sich für staatliche Stellen, die Sicherheitsunbedenklichkeitsbescheinigungen ausstellen, ein vermehrter Bedarf an transparenten Kriterien ergeben, die in den Bestimmungen noch nicht zufriedenstellend enthalten waren. An der Arbeitsgruppe des Normungskomitees 246 („Societal Security“) am *Austrian Standards Institute,* die die ÖNORM S2450 („Umgang mit klassifizierten Informationen-Anforderungen an den Schutz von Verschlusssachen“) ausgearbeitet hat, waren daher unter Vorsitz des Bundeskanzleramts (Büro der Informationssicherheits-kommission) Experten des Innenministeriums und anderer Ministerien sowie aus Wirtschaft und Wissenschaft beteiligt, um die Ausgewogenheit und Praktikabilität der Norm zu gewährleisten. Die ÖNORM S2450 kann beim *Austrian Standards Institute* bezogen werden. *Siegfried Jachs*