Quelle: Consultix

„Vorhut“ der DS-GVO: IT-Sicherheitsgesetz „IT-SiG“

Neue Security-Vorschriften für KRITIS & Co.

Am 25. Mai tritt die neue Datenschutz-Grundverordnung in Kraft. Weil sie für alle Unternehmen relevant ist, ist sie derzeit in aller Munde. Im Schatten der DS-GVO gilt die neue Verordnung zum IT-Sicherheitsgesetz „IT-SiG“ bereits drei Wochen zuvor. Diese Verordnung ist weniger bekannt, weil ihr hierzulande direkt „nur“ die etwa 1.700 Betreiber Kritischer Infrastrukturen, „KRITIS“, unterliegen. Dabei weitet sich deren Kreis aufgrund der globalen Vernetzung kontinuierlich aus. Faktisch ist die Zahl der betroffenen Unternehmen um ein Vielfaches höher, denn auch Subunternehmen und bestimmte Zulieferer müssen das neue Gesetz einhalten. Im Grunde sollte sich jedes Unternehmen sowohl mit der DS-GVO als auch IT-SiG beschäftigen, denn in nicht allzu ferner Zukunft hängt ohnehin alles mit allem zusammen.

Alles neu machte der Mai. Vor zwei Jahren, im Mai 2016, trat die erste Rechtsverordnung zum IT-Sicherheitsgesetz in Kraft. Es definierte, welche Unternehmen der KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation sowie Ernährung und Wasser darunter fallen. Ein Jahr später folgten die Festlegungen für die Sektoren Gesundheit, Finanz- und Versicherungswesen, sowie Transport und Verkehr. Mit der dritten Stufe am kommenden 3. Mai ist die Einhaltung der Verordnung für alle KRITIS-Betreiber verpflichtend. Sie ist essenzieller Bestandteil der IT-Compliance und unterliegt dem Bundesamt für Sicherheit in der Informationstechnologie, BSI.

Wer genau sind die KRITIS-Unternehmen? In der EU-Richtlinie 2008/114/EG ist das genau definiert. Demnach fällt unter „Kritische Infrastruktur“ die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen ist. Solche Funktionen sind die Aufrechterhaltung von Gesundheit, Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens im Katastrophenfall. Anders gesagt: Bei mutmaßlichem Ausfall dessen, was unserem Leben existenziell Form und Sicherheit gibt, muss die Notversorgung jederzeit gewährleistet sein, um Chaos und mithin die Störung oder gar Zerstörung des staatlichen Ganzen zu verhindern.

So zählen Heizkraftwerke, Krankenhäuser, Energieversorger, die Bahn, aber auch Logistik-Unternehmen klassischerweise zum weiten Feld der KRITIS-Unternehmen. Wer noch genau, kann in der BSI-Kritisverordnung nachgeschlagen werden. Betreiber Kritischer Infrastrukturen sind laut IT-SiG dazu verpflichtet, für diejenigen IT-Systeme, -Komponenten oder -Prozesse, die für den Betrieb der Kritischen Infrastruktur entscheidend sind, angemessene Schutzmaßnahmen zu ergreifen. Dieses sind

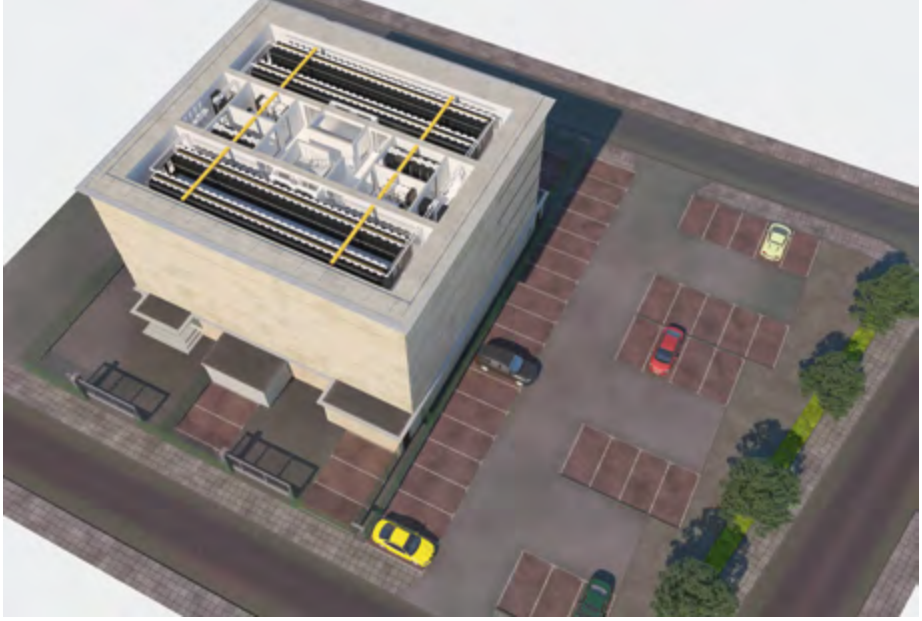
- die Gewährleistung der Sicherheit der Systeme und Anlagen
- das Erkennen, Analysieren und Eindämmen von Sicherheitsvorfällen (SIM)
- die Sicherstellung der Betriebskontinuität (BCM)
- die ständige Überwachung, Überprüfung und Erprobung ihrer IT-Systeme
- die Einhaltung internationaler Normen.

Bedingungen der IT-Sicherheit

Naturgemäß macht der digitale Wandel insbesondere Unternehmen und Kritische Infrastrukturen anfällig für Cyberattacken. Der erste Schritt als KRITIS-Unternehmen ist es daher, eine Risikobetrachtung durchzuführen, um zu eruieren, wo die eigenen Bedrohungen und Schwachstellen sowie die abhängigen Risikofaktoren liegen. Die IT – so schreibt es die BSI-Kritisverordnung vor – muss dabei auf dem „Stand der Technik“ sein; sprich: das hauseigene Netzwerk gesichert, kritische IT-Ressourcen bestimmt und damit die Ausfallsicherheit erhöht sein. Kommt es nämlich an einer Stelle zum Ausfall, darf das nicht den Ausfall des gesamten Systems nach sich ziehen!

Die Verantwortung endet jedoch nicht am Firmenausgang, im Gegenteil: sie setzt sich hier fort. Denn IT-SiG nimmt jedes KRITIS-Unternehmen in die Pflicht, sämtliche Sicherheitsstandards auch auf seine für den Funktionserhalt relevanten Subunternehmen vollumfänglich zu übertragen. Die geforderten Schutzmaßnahmen für den Betrieb der Kritischen Infrastruktur gelten so auch für nachgelagerte Dienstleistungen und Prozesse. Die Anforderungen hinsichtlich der IT-Sicherheit übertragen sich somit von den Betreibern auf deren Subunternehmen. Das ist ein substanzieller Aspekt, der laut BSI bisher aber nur von wenigen KRITIS-Unternehmen bedacht wird. Das Ministerium wünscht sich daher, dass dieser Aspekt der justiziablen Zusammengehörigkeit von Kern- und Subunternehmen zukünftig stärker in den Fokus rücken soll.

Ein Beispiel: Strom- und Treibstoffversorgung, die unter KRITIS fallen, wirken auf andere Branchen. Eine Bank kann sich nicht darauf verlassen, dass die Infrastruktur des Energieversorgers sicher ist. Sie muss kalkulieren, dass es zu einem Ausfall kommt. Für die Bank bedeutet das: Sie muss selbst Vorsorge treffen, um sich KRITIS-konform aufzustellen,



◀ *Beispiel für ein Hochsicherheitsrechenzentrum: Fünf gespiegelte Rechenzentrumsetagen mit je zwei Sicherheitszonen sorgen für unterbrechungsfreien Betrieb. (Quelle: Consultix)*

zum Beispiel mit einer Netzersatzanlage. Beauftragt der KRITIS-Betreiber nun einen Subunternehmer, eine solche Ersatzanlage zu installieren, muss er Sorge tragen, dass dieser entsprechende Sicherheitsvorkehrungen für die IT-Infrastruktur trifft. Umgekehrt müssen auch von Seiten der Subunternehmer Richtlinien erstellt, Konzepte entwickelt und Sicherheitsmaßnahmen festgelegt werden, um den Schutzbedarf zu erfüllen.

Zusätzlich gelten laut BSI künftig auch für Anbieter von digitalen Diensten – wie etwa Online-Marktplätze, Online-Suchmaschinen oder Anbieter von Cloud-Computing-Diensten – erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme. Von dieser Neuregelung sind laut Bundesinnenministerium hierzulande zwischen 500 und 1.500 Unternehmen betroffen. Dadurch verdoppelt sich die Anzahl der von IT-SiG betroffenen Primärunternehmen nahezu. Inklusive der Vielzahl betroffener Subunternehmen erreicht sie leicht sogar einen fünfstelligen Wert.

Lösung Hochsicherheits-Rechenzentren

Die gesetzeskonforme Umsetzung sämtlicher IT-SiG-Regularien stellt für alle betroffenen Unternehmen eine Herausforderung dar. Weil Angriffe auf die globale IT-Architektur immer massiver werden, hat das BSI mit Inkrafttreten des IT-SiG die systematische Kontrolle der KRITIS-Unternehmen angekündigt. Insbesondere für solche, die ihre IT in einem eigenen Rechenzentrum betreiben, ist die vollumfängliche Gewährleistung der IT-Sicherheit und -Verfügbarkeit ein schwieriges Unterfangen. Denn ein großflächiger Stromausfall, Blitz- oder Flugzeugeinschläge, Erdbeben, Hochwasser, Sabotage, Einbruch, Technikmängel oder Feuer sind nur einige der Permanent-Risiken, die für den Ausfall der KRITIS-Sicherheitsstruktur sorgen können. Genau das aber soll qua Gesetz um jeden Preis verhindert werden, um verheerende Folgen für das Leben in Deutschland abzuwenden.

Eine Lösung für KRITIS-Betreiber, die Verfügbarkeit und IT-Sicherheit zu gewährleisten, ist darum, die IT-Infrastruktur wie Datenspeicher und Server in ein hochsicheres Rechenzentrum auszulagern, bevorzugt in Deutschland. Nachweislich müssen solche Hochsicherheits-Rechenzentren risikofrei hinsichtlich sämtlicher physischer Permanent-Risiken sein. Der Kreis relevanter, in Frage kommender Rechenzentren ist in Deutschland sehr überschaubar. Von den gezählten derzeit etwa 5.000 bundesdeutschen Rechenzentren fallen nur wenige unter diesen Anspruchs- und Anforderungslevel. Von den drei Kategorien „kleines", „mittleres" und „großes" Rechenzentren sind es durchweg die mittleren und großen Rechenzentren, die jedes für sich aber noch einmal gesondert betrachtet werden sollten.

Prototypisch wurde zuletzt in Bremen ein mittleres Hochsicherheits-Rechenzentrum in einem ehemaligen Atomschutzbunker des Bundes errichtet. Es wurde für Tier-4/Class-4-Kriterien ausgelegt und durchläuft die ISO-27001-Auditierung. Bewusst wurde der Standort gewählt, weil er zum Beispiel im Vergleich zur Hochburg der Rechenzentren in Deutschland, der Rhein-Main-Region, keinerlei Erdbebentätigkeit aufweist und das Blitzgeschehen signifikant niedriger ist. Dies sind beileibe nicht die einzigen Vorteile. Tatsächlich gehen die Ausfälle von Rechenzentren durch Naturgewalten europaweit in die Milliarden Euro. KRITIS-Unternehmen vertragen keinerlei Ausfälle. Der ehemalige Bremer Atomschutzbunker verfügt sowohl über Housing, Colocation, Private-Cloud-Infrastrukturen als auch flexible Anbindungen an Public-Cloud-Services wie Amazon, Google oder Azure. Sicherheitsmaßnahmen wie Intrusion Prevention, DDos Attack Mitigation oder Remote Triggered Black Holing RBTH machen das mittlere Rechenzentrum digital faktisch unangreifbar. Alle Prozesse sind sowohl DS-GVO- als auch IT-SiG-konform.

Unternehmens-Kontrollen durch das BSI

KRITIS-nahe Unternehmen sollten sich schnellstmöglich um die IT-Sicherheit ihrer Infrastruktur kümmern. KRITIS-Betreiber haben nicht länger eine Übergangsfrist, wenn im Zuge der neuen Befugnisse des BSI ab 3. Mai auch unangekündigte Kontrollbesuche der Behörde möglich sind. In diesem Fall sind Audits, Prüfungen oder Zertifizierungen zum Nachweis der IT-Sicherheit jederzeit vorzulegen. Zusätzlich zu den Anforderungen sind IT-Störungen grundsätzlich meldepflichtig. Hierzu müssen die Unternehmen dem BSI vorab eine Kontaktstelle nennen. Wer dazu gehört und wer nicht oder noch nicht, ist letztendlich nur eine philosophische Frage. Denn jedes Unternehmen für sich wird naturgemäß äußerst sensibel in der Beurteilung der Sicherheit seiner IT-Struktur sein. Ob KRITIS oder nicht, sind für Unternehmen Outsourcing-Optionen der IT-Infrastruktur in hochsichere deutsche Rechenzentren, Zertifizierungen im Bereich IT-Sicherheit und Datenschutz essenzieller denn je. Im Schatten der DS-GVO bricht sich mit IT-SiG so eine zweite Sicherheits-Komponente Bahn, die nicht nur KRITIS-Unternehmen in besonderer Weise motivieren sollte, ihre IT-Sicherheitsstruktur in das gnadenlose Licht der vorbehaltlosen Überprüfung und Angleichung an den nachvollziehbaren Willen des Gesetzgebers zu stellen. ■

ANDRES DICKEHUT,
CEO Consultix GmbH und Gesellschafter der ColocationIX GmbH