EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Drachen zähmen: KRITIS-Audit

Fachartikel von Stephan Hoster, Head of Business Consulting Germany

Jedes wirtschaftlich handelnde Unternehmen trifft „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen“ aus wohlverstandenem Eigeninteresse. Die Beurteilung der Maßnahmen obliegt dem Unternehmen. Angemessen bedeutet in der Regel „wirtschaftlich sinnvoll“. Bei Unternehmen, die unter das BSI-Gesetz fallen sieht die Angelegenheit etwas anders aus.

Seit 2005 arbeitet die Bundesregierung an der Absicherung der für die Versorgung der Bevölkerung in Deutschland kritischen IT-Infrastruktur (KRITIS). Am 3. Mai 2016 wurde mit dem ersten Teil der BSI-Kritisverordnung (BSI-KritisV)[1] Klarheit zur Umsetzung von BSI-Gesetz und IT-Sicherheitsgesetz geschaffen. Kritische Infrastrukturen sind demnach solche, die 500.000 Einwohner versorgen können. Für die betroffenen Branchen wurde dies in den Anhängen der Verordnung konkreter: so ist zum Beispiel ein Krankenhaus dann eine kritische Infrastruktur, wenn die Fallzahl von 30.000 stationären Fällen[2] pro Jahr erreicht oder überschritten wird.

Die Versorgung muss sichergestellt sein

Den Betreiber einer kritischen Infrastruktur treffen im Wesentlichen zwei Pflichten: a) die Vermeidung von Störungen und b) die Meldung von wesentlichen Störungen an das BSI. Das übergeordnete Ziel ist die Sicherstellung der Versorgung, daher sind getroffene Maßnahmen nicht unter dem Gesichtspunkt der Wirtschaftlichkeit, sondern unter dem Gesichtspunkt der Effektivität bei der Erreichung dieses übergeordneten Ziels zu bewerten. Konkret: „Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht.“

Branchenspezifische Sicherheitsstandards

Ein KRITIS-Audit nach §8a BSI-Gesetz überprüft genau diese Vorkehrungen. Dabei hat der Gesetzgeber erleichternd zugestanden, dass Branchenverbände Leitlinien (sog. „branchenspezifische Sicherheitsstandards (B3S)“) vorlegen und vom BSI genehmigen lassen. Setzt ein betroffenes Unternehmen diese Leitlinien um, und überprüft diese alle zwei Jahre in einem internen Audit, so geht der Gesetzgeber davon aus, dass damit alle Auflagen erfüllt sind.

Zum genannten Beispiel Krankenhaus existiert seit dem 18. Dezember 2018 ein „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus[3]“ der Deutschen Krankenhausgesellschaft

[1] https://www.gesetze-im-internet.de/bsi-kritisv/

[2] BSI-KritisV Anhang 5, Teil 3, Ziffer 1.1

[3] https://www.dkgev.de/media/file/106131.ITSiG_Kritis_B3S_Gesamtdokument.pdf

(DKG). Dieser ersetzt die „Umsetzungshinweise“ der DKG aus 2017 und wird, sobald das BSI zugestimmt hat, zu einem Umsetzungshilfsmittel für Krankenhäuser, die als KRITIS eingestuft sind.

Der Standard empfiehlt im Kern die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 fokussiert auf die kritischen Dienstleistungen in den Funktionsstellen nach ISO 13080. Die Zertifizierung nach ISO 27001 ist nicht erforderlich.

Dadurch reduziert sich der Aufwand für die Krankenhaus-IT deutlich. Als wesentliche **Schritte** verbleiben:

1. Anwendungsbereiche identifizieren
2. Managementstrukturen definieren
3. Organisatorische Rollen umsetzen
4. Meldewesen umsetzen
5. Bedrohungsanalyse durchführen
6. Maßnahmen zur Abwehr definieren
7. Maßnahmen umsetzen
8. Verbesserungsbedarf ermitteln
9. Weiter mit (5)

Inhaltlich ist dabei insbesondere auf die **Kernprozesse** für Informationssicherheit zu achten:

1. Störungserkennung
2. Störungsbehebung
3. Krisenmanagement
4. Berechtigungsvergabe
5. Berechtigungskontrolle
6. Berichtswesen
7. Meldewesen
8. Mitarbeiterschulung

Diese Vorkehrungen tragen zur Vermeidung von Störungen bei und sorgen Fehlentwicklungen vor.

Wie unterstützt die IPG?

IPG unterstützt seit vielen Jahren Unternehmen im Bereich der kritischen Infrastrukturen bei der Verbesserung derer IT-Sicherheit.

Durch die standardisierte IPG-Methodik kann ein ISMS, aufbauend auf eine an ITIL angelehnten IT-Betriebsorganisation, innerhalb von drei Monaten in Betrieb genommen werden (Schritte 1 - 4). Der erste Durchlauf durch Schritte 5 - 8 ist im weiteren Verlauf des ersten Jahres möglich. Anschließend ist der erfolgreiche Durchlauf durch ein KRITIS-Audit ohne Probleme möglich.

Der Kernpunkt jeder Einführung ist die Bedrohungsanalyse (Schritt 5). Dabei werden die **Schutzziele der Vertraulichkeit** (kein unbefugter Zugriff auf Daten), **Integrität** (Unverfälschtheit von Daten) und **Verfügbarkeit** (Möglichkeit des Zugangs zu Daten) beleuchtet und geeignete Maßnahmen zu deren Sicherung und zur Risikoabwehr entwickelt.

Die IT-Berechtigungen stehen im Fokus

Die Beherrschbarkeit der IT-Umgebung gründet dabei wesentlich stärker auf der Kontrolle über die tatsächlichen Berechtigungen als auf der Vorkehrung vor Angriffen.

Wer hat Zugriff auf bestimmte Daten, darf lesen oder ändern, und warum eigentlich? Wer hat das denn erlaubt? Und wann? Gelingt die Kontrolle der Berechtigungen nicht, hat am Ende der Azubi alle Rechte im Unternehmen und sieht alle Daten. Leider auch heute noch allzu häufige Realität in den Unternehmen.

Die Methodik von IPG setzt hier drei eng miteinander verschränkte Elemente dagegen und stellt so die Kontrolle (wieder) her:

1. Rollenbasierte Rechtemodellierung
2. Toolgestützte Vergabe von Berechtigungen über Self-Service-Verfahren mit Genehmigungsprozess
3. Ergänzende Absicherung der Bereiche mit erhöhtem oder hohem Schutzbedarf durch Mehrfaktor-Authentisierung sowie Überwachung und Steuerung privilegierter Zugriffe (eigener oder fremder Mitarbeitenden)

Durch Abarbeitung dieser Schritte der IPG-Methodik, wird die IT moderner Unternehmen ertüchtigt und auf die Anforderungen der KRITIS-Verordnung eingestellt.

IPG verfügt darüber hinaus über interne Auditoren mit „Zusätzlicher Prüfverfahrens-Kompetenz für § 8a (3) BSIG“, die alle zwei Jahre ein KRITIS-Audit vorbereiten und mit dem betroffenen Unternehmen gemeinsam durchführen können.

Klingt das nach Ihrem Drachen? Kontaktieren Sie uns. Wir zähmen ihn gemeinsam.

Christian Rückert: Sales Manager Germany
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Markus Blaha: Sales Manager Austria an Switzerland
markus.blaha@ipg-group.com; Telefon +43 (676) 734 23 00