Prüfung gemäß § 8A BSIG und BSI-KRITISverordnung

HiSolutions unterstützt Sie bei der Umsetzung und dem Nachweis der gesetzlich geforderten Maßnahmen zur Absicherung Ihrer IT-Systeme

Betreiber Kritischer Infrastrukturen sind laut IT-Sicherheitsgesetz dazu verpflichtet, ihre IT abzusichern und die Sicherungsmaßnahmen dem BSI gegenüber gemäß § 8a BSIG alle zwei Jahre nachzuweisen. Klassische Zertifizierungen gemäß ISO 27001 oder BSI IT-Grundschutz reichen dafür nicht aus. Wir unterstützen Sie bei der Prüfungsvorbereitung sowie beim Aufbau des ISMS mit integriertem Krisen- und Notfallmanagement oder Prüfen Ihr bereits etabliertes System.

GRUNDLAGE: IT-SICHERHEITSGESETZ

Das im Juni 2015 verabschiedete IT-Sicherheitsgesetz verpflichtet Betreiber Kritischer Infrastrukturen dazu, alle für die Erbringung kritischer Dienstleistungen erforderlichen IT-Systeme nach dem Stand der Technik abzusichern.

Die Absicherung ist dem BSI gegenüber alle zwei Jahre im Rahmen einer Prüfung gemäß § 8a BSIG nachzuweisen. Dabei sind auch branchenspezifische Sicherheitsstandards zu berücksichtigen.

DIE PRÜFUNG GEMÄß § 8A BSIG

Im Fokus der Prüfung gemäß § 8a BSIG steht die Vermeidung von Versorgungsengpässen und somit das Sicherstellen der Verfügbarkeit der IT-Systeme für kritische Dienstleistungen.

Für die Behandlung von Risiken der Verfügbarkeit sind daher Risikobehandlungsstrategien wie Risikoakzeptanz oder -übernahme nicht ohne weiteres zulässig.

UNSERE LEISTUNGEN

Umfassende Prüfungsvorbereitung:
Unsere Experten begleiten Sie während des gesamten Umsetzungsprozesses. Dies umfasst die Definition des Geltungsbereichs, die Erstellung der Prüfgrundlage, die Durchführung einer GAP Analyse sowie die Ermittlung, Umsetzung und Integration der Maßnahmen.

Informations- und Meldepflicht:
Wir unterstützen Sie bei der Anpassung Ihres ISMS, des Krisen- und Notfallmanagements und der Kommunikationsstrategie.

Technische Audits und Penetrationstests:
Überprüfung und Nachweis der Umsetzung von Maßnahmen nach dem Stand der Technik.

Synergieeffekte nutzen:
Als vom BSI anerkannte prüfende Stelle bietet HiSolutions zudem die Kombination der Prüfung gemäß § 8a BSIG mit BSI IT-Grundschutz oder ISO 27001 an.

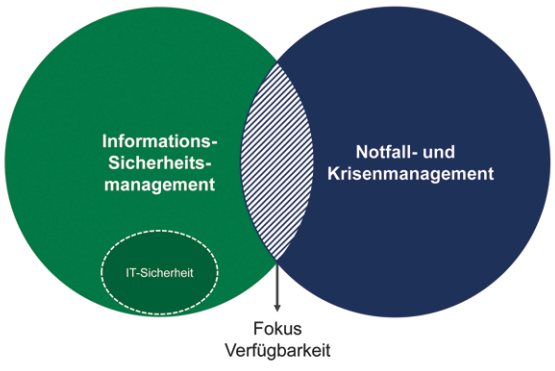

Abb.: Zusammenspiel von Informationssicherheitsmanagement und Notfall- und Krisenmanagement

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

HISOLUTIONS

PFLICHTEN DER BETREIBER

Betreiber Kritischer Infrastrukturen sind demnach dazu verpflichtet, folgende Themen zu berücksichtigen bzw. umzusetzen:

- Melde- und Informationspflicht: Einrichtung einer 24/7 Kontaktstelle zum BSI innerhalb von sechs Monaten
- Identifizierung von kritischen Dienstleistungen und den zugehörigen Anlagen, sowie Prüfung ob der Versorgungsgrad der Anlagen über den definierten Schwellenwerten liegt
- Auflisten Dritter, an welche IT für den Betrieb kritischer Dienstleistungen ausgelagert wurde
- Aufbau oder Anpassung eines ISMS mit integriertem Krisen- und Notfallmanagement
- Entwicklung einer Prüfgrundlage unter Berücksichtigung branchenspezifischer Sicherheitsstandards
- Vermeidung von IT-Störungen durch Umsetzung angemessener organisatorischer und technischer Maßnahmen nach dem Stand der Technik
- Nachjustierung von Risikoübernahme und Risikoakzeptanz bei der Verfügbarkeit
- Auswahl und Beauftragung einer prüfenden Stelle
- Begleitung der Termin- und Prüfungsplanung sowie der Durchführung der Prüfung zusammen mit der prüfenden Stelle
- Durchführung der Prüfung und Einreichen der Nachweisdokumente beim BSI

EMPFOHLENE VORGEHENSWEISE

Für die Umsetzung der Pflichten hat sich folgende Vorgehensweise bewährt.

1. Bestimmung des Geltungsbereichs nach den in der BSI-Kritisverordnung vorgegebenen Definitionen und Schwellenwerten, inklusive Festlegung der Dienstleistungen und zugehörigen Anlagen, welche im Sinne der Verordnung als kritisch einzustufen sind.
2. Abstimmen und Festlegen der Prüfgrundlage mit der prüfenden Stelle. Prüfgrundlage kann eine bestehende BSI IT Grundschutz-Zertifizierung in Kombination mit einem branchenspezifischen Sicherheitsstandard (B3S) sein. Sollte kein B3S verfügbar sein, können bestehende Branchensicherheitsstandards zusammen mit der „Orientierungshilfe B3S" des BSI genutzt werden.
3. Durchführen einer GAP Analyse um die Umsetzung der Maßnahmen zu prüfen sowie um festzustellen, ob diese dem Stand der Technik entsprechen und ob die branchenspezifischen Sicherheitsstandards abgedeckt werden. Prüfen und gegebenenfalls Nachjustieren bestehender Maßnahmen der Risikoübernahme und Risikoakzeptanz
4. Integration der Maßnahmen in das ISMS mit integriertem Krisen- und Notfallmanagement.
5. Prüfung gemäß § 8a BSIG und Übermittlung der Nachweisdokumente an das BSI

Manuel Atug
Head of Business Development

info@hisolutions.com
Fon. +49 30 533 289-0

ÜBER DIE HISOLUTIONS AG

HiSolutions ist einer der führenden Beratungsspezialisten für Information Security, Risikomanagement und Business Continuity Management im deutschsprachigen Raum.

HiSolutions bietet darüber hinaus Schulungen nach § 8a BSIG für Mitarbeiter der Betreiber Kritischer Infrastrukturen an, um diese geeignet auf die Umsetzung und anschließende Prüfung vorzubereiten.

Als vom BSI anerkannte prüfende Stelle bietet HiSolutions zudem die Kombination der Prüfung nach § 8a BSIG mit BSI IT-Grundschutz oder ISO 27001 an.