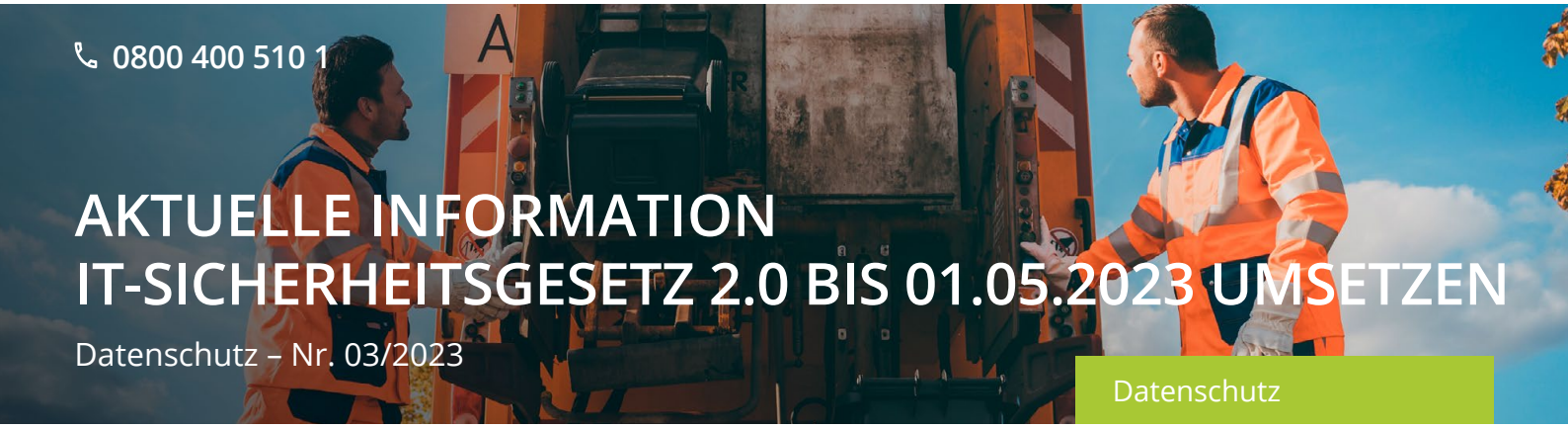


0800 400 510 1

AKTUELLE INFORMATION IT-SICHERHEITSGESETZ 2.0 BIS 01.05.2023 UMSETZEN

Datenschutz – Nr. 03/2023

Datenschutz

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

IT-Sicherheitsgesetz 2.0 und Datenschutzrecht-erweiterte Pflichten für KRITIS-Betreiber und Unternehmen im besonderen öffentlichen Interesse

Das IT-Sicherheitsgesetz 2.0, das am 23.04.2021 als Weiterentwicklung des IT-Sig 1.0 durch den Deutschen Bundestag beschlossen wurde, ist am 28.05.2021 in Kraft getreten (BGBl 2021 Teil I Nr. 25) und begründet **spätestens bis zum 01.05.2023 die Umsetzungspflicht erweiterter Sicherheitsmaßnahmen für die IT-Systeme bei KRITIS-Betreibern und Unternehmen im besonderen öffentlichen Interesse.** Aber auch andere Unternehmen und Organisationen können die empfohlenen Sicherheitsstandards auf freiwilliger Basis nutzen, um das Vertrauen von Partnern und Wirtschaftsprüfern in die IT-Security zu erhöhen.

Neuerungen aus datenschutzrechtlicher Sicht

Um die Informationssicherheit in Deutschland wesentlich zu verbessern und die Cyber-Sicherheitsstrategie der Bundesregierung in ein gesetzlich festgelegtes Fundament zu gießen, so dass Systemausfällen durch Extremfälle wie Systemangriffen oder Shutdowns präventiv begegnet werden kann, wurden konkrete Reformen zur Erhöhung der Sicherheit informationstechnischer Systeme eingeführt, die auch das Datenschutzrecht betreffen. Das BSI hatte bereits im Jahr 2020 einen durchschnittlichen Zuwachs von rund 320.000 neuen Computervirus-Varianten festgestellt, was einen stetigen Anstieg von Cyberangriffen auf Unternehmen anzeigt.

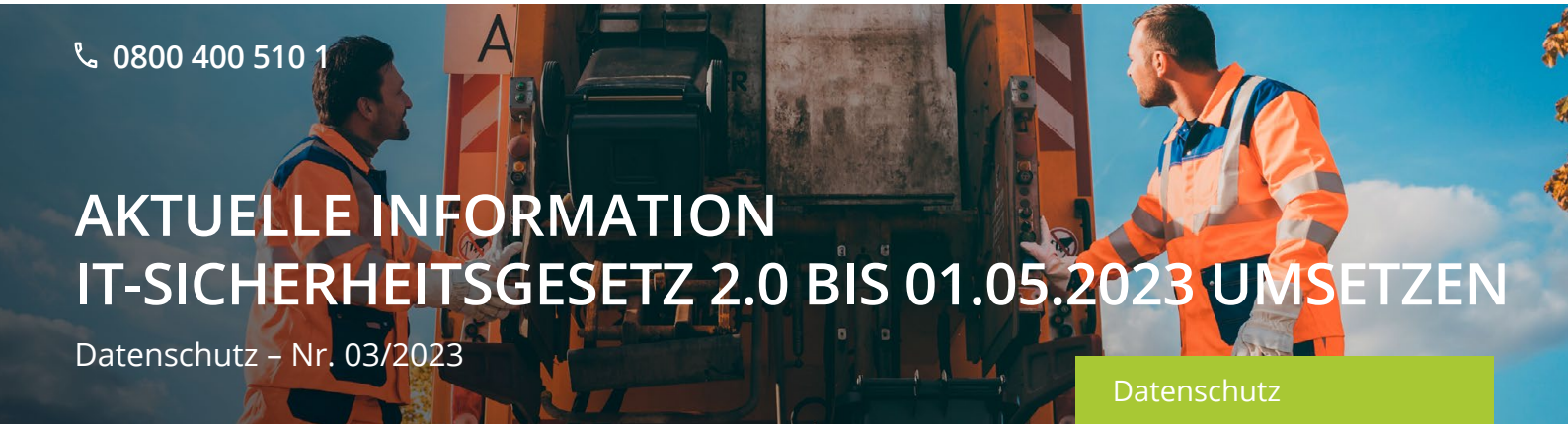
Daher bekommt im Rahmen des IT-Sig 2.0 das Bundesamt für Sicherheit in der Informationstechnik (BSI) weitreichendere Kompetenzen, um die Mindeststandards zum Schutz der IT-Systeme vorschreiben und die Einhaltung derer kontrollieren zu können. Aus datenschutzrechtlicher Sicht darf das BSI künftig innerhalb seiner neuen Kompetenzen etwa im Betrieb von Kommunikationstechnik des Bundes anfallende Protokolldaten im Rahmen der Kommunikation zwischen Bürger und Behörde bis zu 1 ½ Jahre aufbewahren. Außerdem darf das BSI die Herausgabe notwendiger Informationen einschließlich personenbezogener Daten herausverlangen.

Leistungsangebot Datenschutz

- Externer Datenschutzbeauftragter
- Datenschutz - Online Beratung
- Beratung des internen Datenschutzbeauftragten
- Datenschutzaudits & Risikoanalysen
- Datenschutz Dokumentation im Unternehmen
- Datenschutzmanagementsysteme
- Branchenspezifische Datenschutzberatung
- Datenschutzschulungen
- FKC CONSULT - Datenschutzsiegel
- Krisenmanagement

WIE KÖNNEN WIR IHNEN HELFEN?

datenschutzberatung@fkc-gmbh.de



0800 400 510 1

AKTUELLE INFORMATION IT-SICHERHEITSGESETZ 2.0 BIS 01.05.2023 UMSETZEN

Datenschutz – Nr. 03/2023

Datenschutz

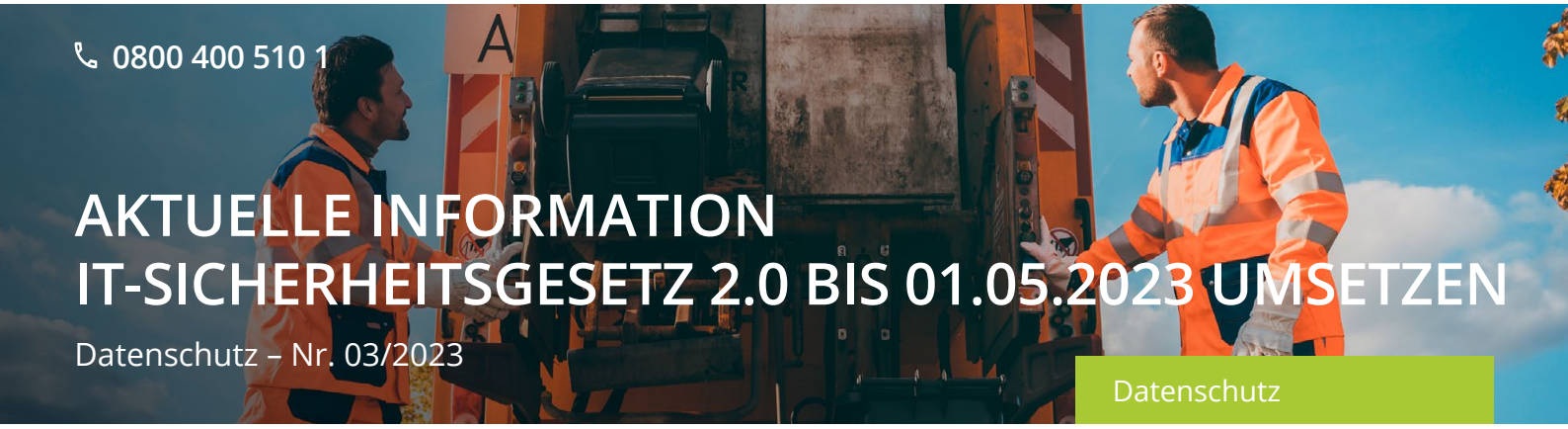
Erweiterter Adressatenkreis des IT-Sig 2.0

Das IT-Sig 2.0 richtet sich an alle KRITIS-Betreiber und ergänzt die Kategorie „Unternehmen im besonderen öffentlichen Interesse“. Zu den KRITIS-Betreibern gehören Unternehmen und Organisationen, die unentbehrlich für das staatliche Gemeinwesen sind und durch deren Ausfall die öffentliche Sicherheit gefährdet wäre.

In Deutschland zählen die Sektoren Abfallwirtschaft (neu im IT-Sig 2.0), Ernährung, Staat und Verwaltung, Energie, Gesundheit, IT und TK, Transport und Verkehr, Medien und Kultur, Wasser, Finanzen und Versicherungen zu den KRITIS-Betreibern.
Zu den „Unternehmen im besonderen öffentlichen Interesse“ gehören diejenigen, die von „erheblich volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind. Daher sollten Unternehmen, die nicht unbedingt zu den bereits oben erwähnten Sektoren zählen, genau prüfen, ob sie nicht zu den Unternehmen im besonderen öffentlichen Interesse angehören und sich daher aus dem IT-Sig 2.0 neue Pflichten für sie ergeben könnten.

Zusammenfassung der neuen Pflichten und Reformen

- Bis spätestens zum 01.05.2023 sind besondere Systeme zur Angriffserkennung verpflichtend zu implementieren, deren Funktionsfähigkeit in KRITIS-Prüfungen nachweisbar sein muss.
- KRITIS-Betreiber müssen sich beim BSI registrieren und bei Störungen alle Informationen einschließlich personenbezogener Daten zur Beseitigung des Störfalls an das BSI herausgeben.
- Alle informationstechnischen Systeme sind auf den neuesten Stand der Technik zu bringen, deren Nachweis über Sicherheitsaudits, Prüfungen und Zertifizierungen, z. B. nach ISO 27001 erbracht werden kann.
- Neue, freiwillige IT-Sicherheitskennzeichen geben Aufschluss über die Sicherheitseigenschaften einen Produkts der jeweiligen Unternehmen und können dem BSI mitgeteilt werden, das die Sicherheitskennzeichen auf die vorgeschriebenen Vorgaben überprüft.



0800 400 510 1

AKTUELLE INFORMATION IT-SICHERHEITSGESETZ 2.0 BIS 01.05.2023 UMSETZEN

Datenschutz – Nr. 03/2023

Datenschutz

Höhe der Bußgelder bei Nichteinhaltung

Bei Nichteinhaltung der gesetzlichen Vorgaben nach IT-Sig 2.0 sind die Bußgelder in konkrete Stufen eingeteilt, die von 100.000 bis 2 Mio. Euro reichen können und entsprechend den spezifischen Rahmenbedingungen bis zur Verzehnfachung des Maximalbetrags auf 20 Mio. Euro erhöht werden können.

Umsetzungsmaßnahmen zur Erfüllung der Informationssicherheit:

- Systeme zur Angriffserkennung sind sogenannte Intrusion Detection Systeme, die auf Algorithmen basieren, die anhand von Log-Dateien Angriffe auf Computer, Server und Netzwerke aufspüren. Diese Log-Dateien müssen durch die Unternehmen nicht nur aufgezeichnet, sondern auch ausgewertet werden.
- Reaktionspläne und Präventivmaßnahmen müssen über ein detailliertes Business Continuity Planning und eine Desaster-Recovery-Plan bereitgestellt werden.
- Die System-Absicherung muss dem BSI alle zwei Jahre über ein Audit nachgewiesen werden

Fazit

Alle KRITIS-Sektoren und Unternehmen im besonderen öffentlichen Interesse sind per Gesetz dazu verpflichtet, die Neuerungen des IT-Sig 2.0 **bis spätestens zum 01.05.2023 umzusetzen**. Aber auch andere Unternehmen und Organisationen können die empfohlenen Sicherheitsstandards auf freiwilliger Basis nutzen, die das Vertrauen der Partner und Wirtschaftsprüfer in die IT-Security erheblich steigern würde.

Die Nachweise über die Umsetzung der Informationssicherheit werden üblicherweise über Audits und Zertifikate nach ISO 27001 erbracht.
Wenn Sie als Unternehmen eine Zertifizierung anstreben, wenden Sie sich an uns. Wir begleiten Sie auf dem Weg zur Zertifizierung und führen interne Audits durch.

datenschutzberatung@fkc-gmbh.de

Bilder von Canva.