secunet

IT-Sicherheitsgesetz 2.0

Seit 2015 trägt das IT-Sicherheitsgesetz der Bundesregierung dazu bei, Unternehmen, die Bevölkerung und Behörden vor Cyber-Angriffen zu schützen. 2021 hat dieses Gesetz mit der Version 2.0 ein Update bekommen: Das sollten Betreiber kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse (UBI) jetzt wissen.

secunet.com

Die Änderungen auf einen Blick.

Die Bundesregierung reagiert auf die fortschreitende Digitalisierung. Deshalb beinhaltet die Gesetzesnovelle unter anderem neue Kompetenzen für das Bundesamt für Sicherheit in der Informationstechnik (BSI) und bedeutet für viele Unternehmen, dass sie ihre Sicherheitsstrategie anpassen müssen.

2015
IT-SiG 1.0

2019
erster Entwurf für das IT-SiG 2.0

2020
weitere Konkretisierung

2021
Inkrafttreten des IT-SiG 2.0

01.05.2023
Frist zur Umsetzung der neuen Vorgaben

Erweiterte Kompetenzen für das BSI:

- Kann bei bestimmten Gefahren konkrete Maßnahmen anordnen
- Ist zuständig für KRITIS-Unternehmen und Unternehmen im besonderen öffentlichen Interesse
- Wird zur Kontroll- und Prüfinstanz der Bundesverwaltung
- Darf anonymisierte Protokollierungsdaten 1 Jahr speichern
- Darf bei Telekommunikationsdiensten Bestandsdaten abfragen
- Ist berechtigt, jegliche IT-Produkte auf ihre Sicherheit zu untersuchen
- Ist zuständig für Verbraucherschutz (IT-Sicherheitskennzeichen)

>800

neue Stellen im BSI

Geldbußen von bis zu

€20Mio.

Wen betreffen die Änderungen im IT-SiG 2.0?

Die neuen, gesetzlichen Vorgaben richten sich nicht nur an KRITIS-Betreiber, sondern jetzt auch an Unternehmen im besonderen öffentlichen Interesse.

Jetzt zusätzlich betroffene Unternehmen:

Neu: Das IT-SiG 2.0 erweitert den Geltungsbereich innerhalb der KRITIS-Unternehmen um den Sektor **Siedlungsabfallentsorgung**.

Neu: Eine weitere Gruppe von Unternehmen wird in der Gesetzesnovelle neben den KRITIS-Betreibern jetzt zusätzlich angesprochen: **Unternehmen im besonderen öffentlichen Interesse**. Dazu zählen zum Beispiel Störfallbetriebe und Unternehmen von erheblicher volkswirtschaftlicher Bedeutung.

Bereits mit dem IT-SiG 1.0 angesprochen:

Betreiber kritischer Infrastrukturen in den Bereichen:

Energie

Elektrizität, Gas, Mineralöl, Fernwärme

Wasser

Wasserversorgung, Abwasserbeseitigung

Ernährung

Herstellung und Behandlung von Lebensmitteln, Ernährungswirtschaft, Lebensmittelhandel

Informationstechnik und (andere) Telekommunikation

Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung

Transport und Verkehr

Luftverkehr, Schienenverkehr, Binnen- und Seeschifffahrt, Straßenverkehr, Öffentlicher Personennahverkehr, Logistik, Wetter und Satellitennavigation

Gesundheit

Krankenhäuser, Hersteller von Arzneimitteln und Impfstoffen, Forschungseinrichtungen uvm.

Was ändert sich mit dem IT-SiG 2.0 konkret für die betroffenen Unternehmen?

Für die Unternehmen bedeutet dieses Gesetz, dass sie im Bereich der IT-Sicherheit stärker in die Pflicht genommen werden.

Die Pflichten im Überblick:

1 NEU

Sicherheitsrelevante Netz- und Systemkomponenten dürfen nur von vertrauenswürdigen Herstellern stammen.

2 NEU

Ab dem 01.05.2023 müssen Systeme zur Angriffserkennung im Einsatz sein.

3

Pflicht zur Registrierung einer Kritischen Infrastruktur beim BSI.

4

Pflicht zur Vorlage der für eine Bewertung aus Sicht des BSI erforderlichen Unterlagen und zur Erteilung von Auskunft.

5

Pflicht zur Meldung von IT-Störungen oder erheblichen Beeinträchtigungen.

6

Immer up-to-date: Umsetzung der IT-Sicherheit muss gemäß dem „Stand der Technik“ erfolgen.

7

Alle 2 Jahre Nachweis des Mindestniveaus durch Sicherheitsaudits, Prüfungen oder Zertifizierungen.

Das können Sie jetzt tun, um bestens vorbereitet zu sein.

1 **Wo steht Ihr Unternehmen und was sind die nächsten Schritte?**

Lassen Sie sich individuell beraten und Ihre Ausgangslage analysieren.

2 **Was sind die Bedürfnisse Ihres Unternehmens?**

- Müssen Sie die Anforderungen gemäß Angriffserkennungen erfüllen, um IT-SiG 2.0-konform zu sein?
- Möchten Sie Ihre Systeme und Anlagen absichern und Angriffe auf Ihr System frühzeitig erkennen?
- Die IT-Infrastruktur Ihres Unternehmens soll rundum abgesichert werden?
- Cloud – aber sicher: Sie möchten ein geschütztes Arbeiten in der Cloud ermöglichen?
- Sie sind auf der Suche nach einem Schutzkonzept und/oder Produkte für die Erzeugung, Nutzung und Verwaltung digitaler Zertifikate?

Mit Beratungs- und Produktexpertise an Ihrer Seite.

secunet monitor

IT-SiG 2.0-konforme **Angriffserkennung und -abwehr**

secunet eID PKI Suite

Geschützte **Erzeugung, Nutzung und Verwaltung digitaler Zertifikate.**

secunet edge

IIoT-Gateway, Edge-Computing-Plattform und Firewall mit Netzwerküberwachung in Einem.

SINA

Verarbeitung **schützenswerter Informationen.**

Sicheres **Arbeiten in der Cloud.**

stashcat®

Sicheres und einfach bedienbares **Messaging für die interne Kommunikation.**

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 700 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im Segment Prime Standard der Frankfurter Wertpapierbörse gelistet und erzielte 2021 einen Umsatz von rund 337 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

Weitere Informationen finden Sie unter www.secunet.com.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com