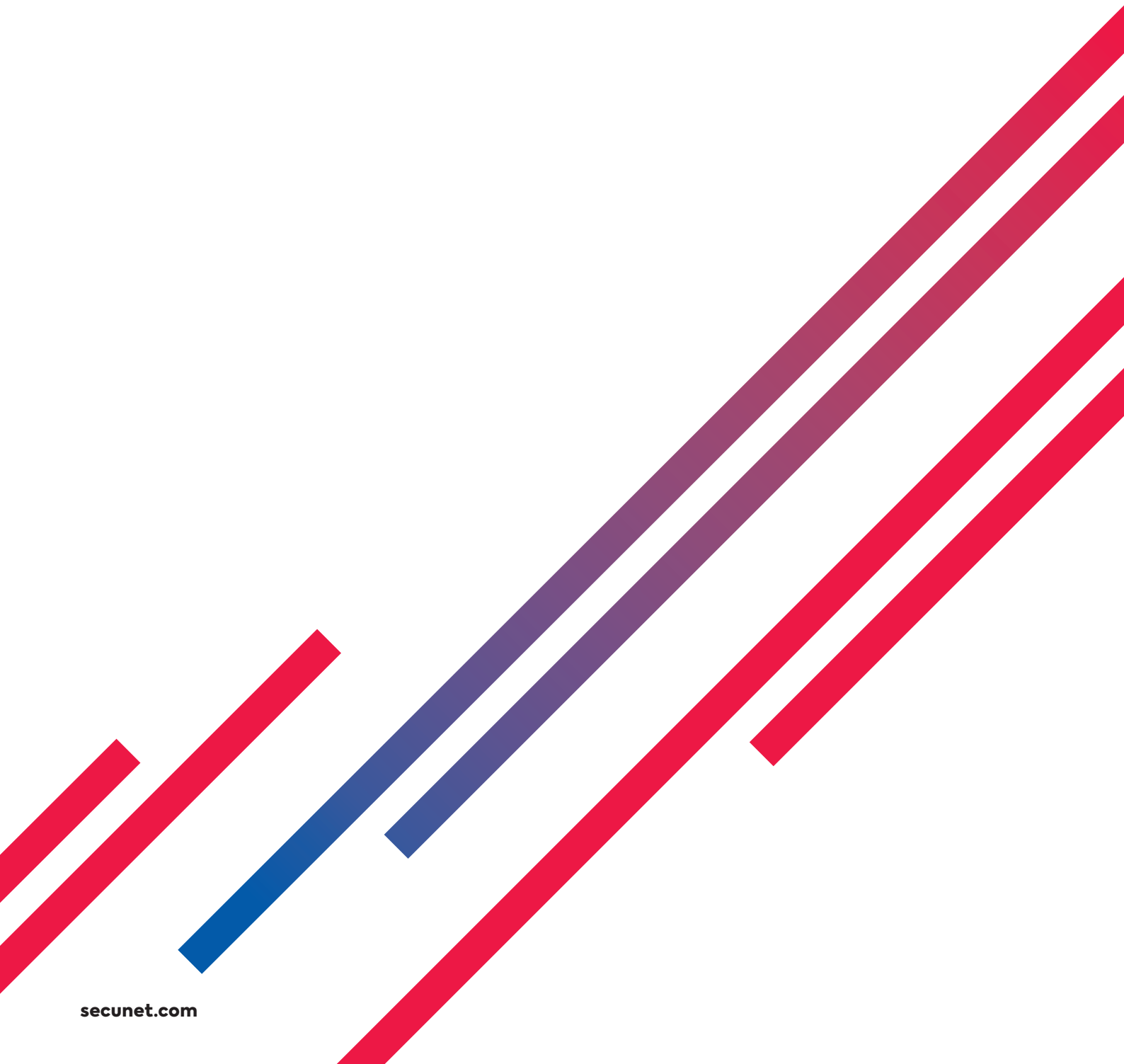
secunet

IT-Sicherheits-gesetz 2.0

Ein Leitfaden für KRITIS-Unternehmen.



Die Änderungen auf einen Blick.

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

Die Orientierungshilfe des BSI konkretisiert die technischen Voraussetzungen der einzusetzenden Systeme zur Angriffserkennung.

2015
IT-Sicherheitsgesetz 1.0

2019
erster Entwurf für das IT-Sicherheitsgesetz 2.0

2020
weitere Konkretisierung

2021
Inkrafttreten des IT-Sicherheitsgesetz 2.0

2022
Veröffentlichung Orientierungshilfe durch BSI

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-Sicherheitsgesetz 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-Sicherheitsgesetz 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-Sicherheitsgesetz 1.0 angesprochen:

Betreiber Kritischer Infrastrukturen in den Bereichen:

Energie
Elektrizität, Gas, Mineralöl, Fernwärme

Wasser
Wasserversorgung, Abwasser-beseitigung

Ernährung
Herstellung und Behandlung von Lebensmitteln, Ernährungs-wirtschaft, 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, Herstellung von Arzneimitteln und Impfstoffen, Forschungseinrichtungen uvm.

Was ändert sich mit dem IT-Sicherheitsgesetz 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 Netzund 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 erforderlichen Unterlagen für die BSI-Bewertung 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 IT-Sicherheitsgesetz 2.0 und die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Was Unternehmen jetzt wissen müssen

Wie ist die „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (OH-SZA) entstanden?

- Das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) betrifft mehr Unternehmen (u.a. Entsorger) im Vergleich zur ersten Fassung, verschärft die Sanktionen, erteilt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mehr Befugnisse und definiert neue Pflichten für KRITIS-Betreiber.
- Die exakten Anforderungen an die einzusetzende Technik werden jedoch nicht ausformuliert. Es werden lediglich Empfehlungen für die Umsetzung der Angriffserkennung ausgesprochen.
- Zu den neuen Pflichten gehört u.a. die Nutzung von technischen Werkzeugen und organisatorischen Prozessen, die zur Erkennung von Angriffen auf informationstechnische Systeme beitragen.
- Die Erkennung soll durch den Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgen.
- Ab dem 1. Mai 2023 ist der Einsatz solcher Systeme verpflichtend und im Rahmen von Audits nachzuweisen.
- Im Juni 2022 veröffentlichte das BSI einen Entwurf der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung.
- Mit der Orientierungshilfe will das BSI die technischen Voraussetzungen der einzusetzenden „Systeme zur Angriffserkennung“ konkretisieren.

Ist die Orientierungshilfe verpflichtend für Unternehmen?

- Die Orientierungshilfe dient als Leitfaden für eine gesetzeskonforme Umsetzung des IT-Sicherheitsgesetzes 2.0.
- Sie bietet damit die maßgebliche Grundlage für die Bewertung durch Auditoren.
- Der Einsatz von entsprechenden Systemen, oder zumindest die detaillierte Planung der Implementierung solcher, ist dem Auditor ab Mai 2023 nachzuweisen. Ist dies den Unternehmen nicht möglich, drohen ihnen hohe Bußgelder.

»

secunet
monitor KRITIS

Was beinhaltet die Orientierungshilfe?

- Anforderungen für die Umsetzung der Angriffserkennung in den drei Bereichen: Protokollierung, Erkennung und Reaktion.
- Im Rahmen dieser Bereiche wird zwischen Muss-, Soll- und Kann-Anforderungen differenziert, wobei die Muss-Anforderungen im ersten Prüfzyklus ab dem 1. Mai 2023 verpflichtend sind.

Welche Muss-Anforderungen werden u.a. vorgeschrieben?

- Eine Angriffserkennung mittels Signaturen bzw. Indicators of Compromise (IOCs)
- Protokollierungsdaten müssen gesammelt, gefiltert, normalisiert, aggregiert und korreliert werden, um sie anschließend für die Auswertung bereitzustellen.

Welche Anforderungen sind optional?

- Einbindung in ein „Security Information and Event Management“ (SIEM) System
- Initiale Kalibrierung über Baselining oder Anomalieerkennung ist nicht unter den Muss-Anforderungen gelistet und wird dementsprechend im ersten Prüfzyklus nicht zwingend benötigt.

Was können Unternehmen jetzt tun?

- Die Komplexität des Themas sorgt bei betroffenen Unternehmen für Unsicherheiten bezüglich der einzusetzenden Mittel und Prozesse. Ein kompetenter Partner kann Firmen dabei einen Überblick verschaffen und helfen, diese Herausforderung zu meistern.
- Mit einer langjährigen Beratungsexpertise im KRITIS-Bereich kann secunet Security Networks AG als führendes IT-Sicherheitsunternehmen Hilfestellung leisten, u.a. durch eine gezielte und individuelle Beratung zum Thema IT-Sicherheitsgesetz 2.0 und die Orientierungshilfe.
- Zudem bietet secunet eine technische Lösung für Unternehmen jeder Größe, welche den Integrations- und Betriebsaufwand auch für kleinere KRITIS-Unternehmen geringhält und sich zielgenau auf die geforderten Mindestanforderungen aus der Orientierungshilfe fokussiert. Dabei wird besonderes Augenmerk auf die Nutzbarkeit für Verantwortliche und die einfache Integration für Dienstleister gelegt.

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-Sicherheitsgesetz 2.0-konform zu sein?
- Möchten Sie Ihre Systeme und Anlagen absichern und Angriffe auf Ihr System frühzeitig erkennen?

Mit Beratungs- und Produktexpertise an Ihrer Seite.

secunet monitor

System zur Angriffserkennung

secunet monitor KRITIS

Netzwerk-Monitoring-System auf Basis signaturbasierter Angriffserkennung. Optimiert für KRITIS-Betreiber.

Weitere Informationen: www.secunet.com/industrie

Kontakt: info@secunet.com

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 1000 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 SDAX 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.

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