TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT "IT-Sicherheitsrechtstag 2021"

Berlin, 24.09.2021

Praktische Herausforderungen des IT-SiG 2.0 für Technologielieferanten

Frank Hülle, Björn Huber-Puls, secunet

secunet

Praktische Herausforderungen des IT-SiG 2.0 für Technologie-lieferanten

24.09.2021 | IT-Sicherheitsrechtstag 2021

Vorstellung

Björn Huber-Puls

Senior Berater Informationssicherheit

Management Systems & Audit

- Beratung zur Informationssicherheit nach BSI IT-Grundschutz und DIN ISO IEC 27001
- Beratung zu Security Awareness
- Erstellung von Sicherheitskonzepten
- Projektmanager gem. GPM IPMA Level C
- Oberstleutnant der Reserve

Vorstellung

Frank Hülle

Senior Berater Informationssicherheit

Management Systems & Audit

- Beratung zur Informationssicherheit nach BSI IT-Grundschutz und DIN ISO IEC 27001
- Beratung zu Security Awareness
- Erstellung von Sicherheitskonzepten
- Schwerpunkt IT-Infrastruktur

Agenda

01 Cyber-Sicherheitslage

02 IT-SiG 2.0 – neue Anforderungen und Handlungsmöglichkeiten

03 Konkrete umzusetzende Anforderungen aus dem IT-SiG 2.0 für Technologielieferanten

04 Herausforderungen und Chancen

01

Cyber-Sicherheitslage

Ausgangssituation: Alte Systeme, neue Risiken

- Der Vernetzungsgrad der Industrie wächst, doch der Austausch der Daten bleibt schwierig. In Fabriken können **„babylonische“ Verhältnisse** herrschen: Maschinen kommen von unterschiedlichen Herstellern, die man kaum miteinander vernetzen kann.
- Bei der Entwicklung industrieller Altsysteme wurden aktuelle Sicherheitsaspekte und Cyber-Bedrohungen nur bedingt berücksichtigt. Ihre teilweise **unklaren Strukturen** sowie offenen Kommunikationskanäle können erhebliche Sicherheitsrisiken aufweisen.
- Je komplexer die Maschinen-, IT-/OT-Landschaft ist, umso anfälliger sind Unternehmen für Cyberangriffe – die **Anzahl der Angriffe sowie deren Schadenshöhe können rasant steigen.**

Ausgangssituation: Gefährdungslage (2020)

322.000
pro Tag

117,4 Millionen neue Schadprogramm-Varianten 2020 (2019: 114 Millionen)

+15 %

mehr erfasste Fälle an Cyberkriminalität in Deutschland **im Jahr 2019 (100.000)** im Vergleich zu 2018

68 %

aller **Automobilhersteller** waren von 2016 bis 2018 von **Datendiebstahl, Sabotage und Industrie-spionage** betroffen. **22 weitere Prozent** vermuten, betroffen zu sein, wissen es aber nicht.

Kritis-Meldungen

76 %

Spam gemessen an allen 2020 in den Netzen des Bundes erhaltenen Mails

>22 Mrd.

Datensätze wurden von **Januar bis Oktober 2020 offengelegt.** Sie stammen **aus 730** veröffentlichten **Datenpannen.**

Ausgangssituation: Gefährdungslage

INTERNETSICHERHEIT

Hackerangriff auf Microsoft: Tausende Mittelständler in Deutschland könnten betroffen sein

KRITISCHE INFRASTRUKTUR

Wasserversorgung durch Hackerangriffe gestört

en Hackerangriffe in Deutschland noch nicht zu Ausfällen

HACK

Ransomware verlangt 50 Millionen US-Dollar von Acer

Acer soll das bisher höchste Lösegeld für einen Ransomware-Angriff bezahlen - sonst könnten interne Daten veröffentlicht werden.

Der weltgrößte Fleischkonzern JBS aus Brasilien hat Cyber-Kriminellen beim Hacker-Angriff, der vergangene Woche die Produktion in Nordamerika und Australien lahmlegte, ein hohes Lösegeld gezahlt. Das Unternehmen bestätigte am späten Mittwoch über seine US-Tochter die Zahlung einer Summe im Wert von 11 Millionen Dollar, umgerechnet 9 Mio Euro.

8. Januar 2020, 18:56 Uhr Direktbank

Hacker-Angriff auf DKB

Nach einem Angriff auf den Server-Dienstleister der Deutschen Kreditbank (DKB) war die Online-Banking-Funktion am Dienstagnachmittag mehrere Stunden gestört. Erst am späteren Abend gelang es der Direktbank-Tochter der BayernLB den Dienst wieder herzustellen. Es könne aber weiter zu Einschränkungen kommen, sagte

WIBATTACK

Weiterer SMS-Angriff auf die SIM-Karte

Wie Simjacker kann auch die Schadsoftware Wibattack Daten aus dem Mobiltelefon ausleiten. Auch hier kommt die Schadsoftware per SMS und läuft auf der SIM-Karte, sie nutzt allerdings eine andere Sicherheitslücke.

30. September 2019, 18:56 Uhr, Moritz Tremmel

Deutsches

Locky meldet sich mit massiven Angriffen auf Krankenhäusern zurück

Die Abzocke mit Covid-19 boomt

Hacker nutzen Homeoffice aus

Corona-Schub für Cyberversicherungen

Stand: 19.10.2020 12:44 Uhr

Viele Menschen arbeiten wegen Corona im Homeoffice. Ihre dortigen Rechner sind oft schlechter geschützt als im Büro. Hackerangriffe nehmen zu. Cyberversicherungen für solche Fälle boomen.

SOLARWINDS-HACK

Ein Hackerangriff, der um die Welt geht

Der Angriff auf das Unternehmen SolarWinds gilt als größter Hack seit Jahren. Zehntausende Firmen könnten betroffen sein. Um was geht es, wie gefährlich ist es und wie kann man sich schützen? Antworten auf die wichtigsten Fragen.

Düsseldorf

Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

22. September 2020, 11:28 Uhr / Quelle: ZEIT ONLINE, dpa, and / 172 Kommentare

0 du Betrügerische

Dieses Jahr sind mehr Geschenke mit der Post unterwegs [illegible] Kriminelle. Sie versuchen, mit gefälschten Benachrichtigungen per Mail Beispiel Kontodaten abzufischen.

17.12.2020, 16.03 Uhr

Ein Tank von Colonial Pipeline. Foto: AP/Seth Wenig

New York. Der Pipeline-Betreiber Colonial Pipeline ist Ziel eines Angriffs mit einem Erpressungstrojaner geworden. Die Pipeline wurde deswegen vorübergehend stillgelegt. Nun sollen die Hacker fünf Millionen Dollar Lösegeld bekommen haben.

HACKER-ANGRIFFE

Mittelständler im Fadenkreuz von Cyber-Kriminellen

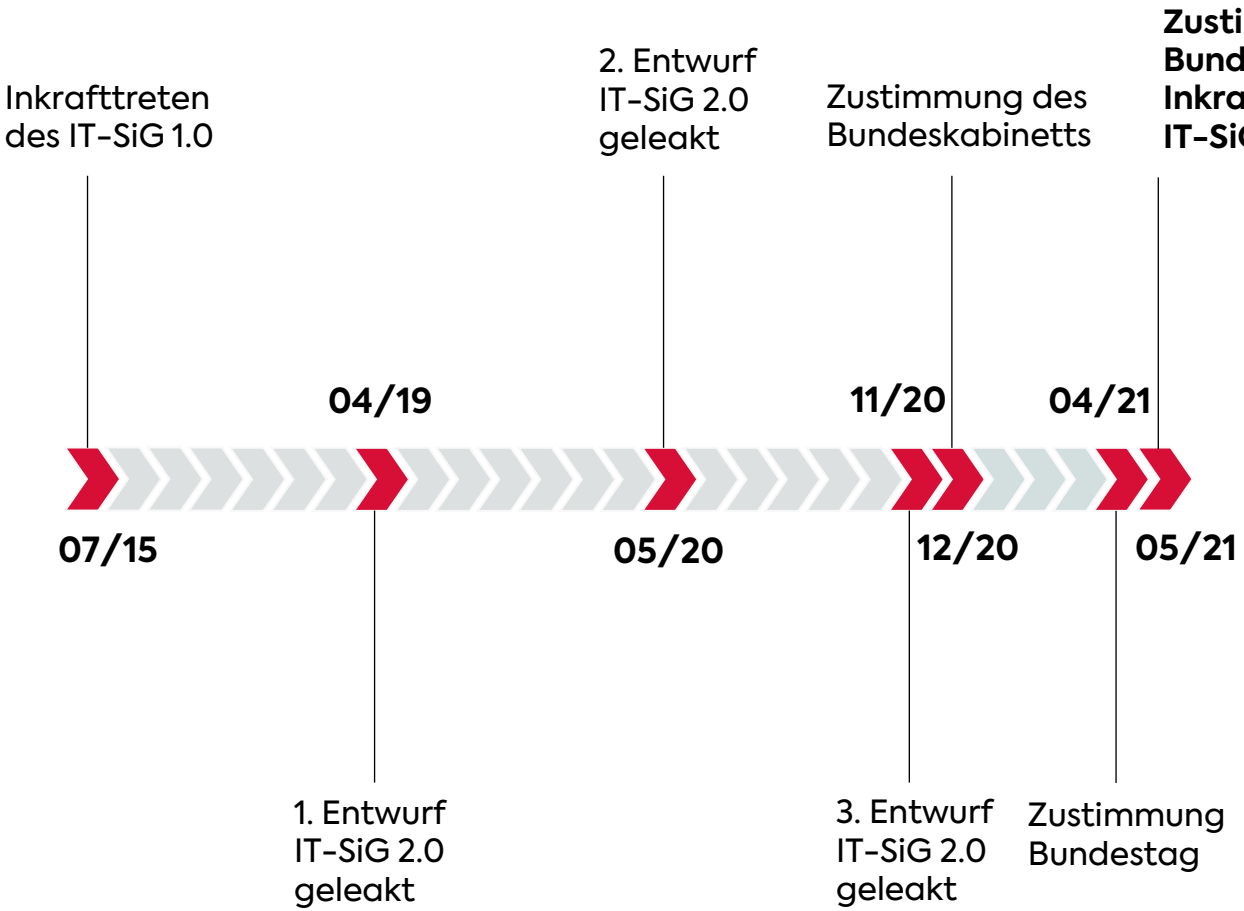
Hacker suchen immer öfter gezielt nach IT-Schwachstellen: Der Anteil der Cyber-Angriffe, bei denen Kriminelle die individuellen Schwachstellen von kleinen und mittleren Unternehmen ausnutzen, steigt deutlich an. Das zeigt eine Auswertung aktueller Schadenstatistiken des Wiesbadener Versicherers R+V.

02

IT-SiG 2.0

Neue Anforderungen und
Handlungsmöglichkeiten

IT-SiG 2.0
Zeitlicher Ablauf



- Das Bundesministerium des Innern hat eine Änderung zum bestehenden IT-Sicherheitsgesetz erarbeitet (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme)
- Auswirkungen auf KRITIS-Unternehmen und Hersteller gegeben
- Bundestag und Bundesrat haben das IT-SiG 2.0 gebilligt, so dass es am 28.05.2021 in Kraft getreten ist
- Die novellierte BSI-KRITIS-Verordnung tritt zum 01.01.2022 in Kraft

IT-SiG 2.0
Kontext und Auswirkungen

Adressiert Bedrohungen für die Cybersicherheit für **Staat, Wirtschaft** und **Gesellschaft**

Auswirkung auf folgende Gesetze und Verordnungen:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Gesetz über die Elektrizitäts- und Gasversorgung (EnWG)
- Außenwirtschaftsverordnung
- Zehnte Buch Sozialgesetzbuch (SGB X)

Änderungen im IT-SiG

Fünf Themen-Gruppen, davon drei im Fokus für Technologielieferanten

BSI-Befugnisse

Weitere Aufgaben und **Kompetenzen** z. B.:

- Suche nach Sicherheitslücken
- Detektion von Risiken
- Sammlung von Informationen über Sicherheitsrisiken
- Festlegung von Mindeststandards

Betroffenheit

Weitere **betroffene Unternehmen** inkl. Erweiterung der Ihnen auferlegten Pflichten:

- Abfallentsorgung
- Infrastrukturen im besonderem öffentlichen Interesse
- Anbieter von Telekommunikations-diensten

Herstellerpflichten

Verpflichtung von **Herstellern** von **IT-Komponenten**

- Für Produkte mit hoher Bedeutung für das Funktionieren des Gemeinwesens
- Vertrauenswürdig-keitserklärung über Lieferkette
- Definition von Mindeststandards durch das BSI

Verbraucherschutz

BSI erhält weitere Kompetenzen bzgl. Verbraucherschutz

- Einführung eines IT-Sicherheits-kennzeichens
- Warnung vor Sicherheitslücken, Schadprogrammen und unerlaubten Datenzugriffen sowie die Empfehlung von Vorkehrungen und Gegenmaßnahmen

Bußgeld

Erhöhung der **Bußgelder:**

- Erhöhung der Bußgeldrahmen bis zu 20 Mio. €
- Erweiterung der Kataloge zu Bußgeldtatbeständen

Erweiterung des Kreises der Betroffenen
Ein weiterer KRITIS-Sektor

Erweiterung des Kreises der Betroffenen
Unternehmen im besonderen öffentlichen Interesse

- **Hersteller und Entwickler**
  - von Gütern der **Kriegswaffen**liste (Teil B)
  - von **Produkten** oder wesentlicher Komponenten mit IT-Sicherheitsfunktionen zur Verarbeitung von **staatlichen Verschlusssachen**
- **Größte Unternehmen in Deutschland**
  (nach inländischer Wertschöpfung)
- **Betreiber im Sinne der Störfallverordnung**
  (Betriebsbereich der oberen Klasse, oder gleichgestellte)

Anforderungen und Handlungsmöglichkeiten
Gruppe 2: Betroffenheit

Betroffenheit	Lösungsmöglichkeiten 
Weitere **betroffene Unternehmen** inkl. Erweiterung der ihnen auferlegten Pflichten ▪ Siedlungs-Abfallentsorgung ▪ Infrastrukturen im besonderem öffentlichen Interesse ▪ Anbieter von Telekommunikations-diensten	▪ Prüfung der Betroffenheit • Definition des Anwendungsbereichs • Durchführung einer GAP-Analyse • Erstellung eines Umsetzungsplans (SdT; ISMS und BCMS; schließen von bekannten Lücken)

Änderungen im IT-SiG
Gruppe 3: Herstellerpflichten

BSI-Befugnisse

Weitere Aufgaben und **Kompetenzen** z. B.:

- Suche nach Sicherheitslücken
- Detektion von Risiken
- Sammlung von Informationen über Sicherheitsrisiken
- Festlegung von Mindeststandards

Betroffenheit

Weitere **betroffene Unternehmen** inkl. Erweiterung der ihnen auferlegten Pflichten:

- Abfallentsorgung
- Infrastrukturen im besonderem öffentlichen Interesse
- Anbieter von Telekommunikations-diensten

Herstellerpflichten

Verpflichtung von **Herstellern** von **IT-Komponenten**

- Für Produkte mit hoher Bedeutung für das Funktionieren des Gemeinwesens
- Vertrauenswürdig-keitserklärung über Lieferkette
- Definition von Mindeststandards durch das BSI

Verbraucherschutz

BSI erhält weitere Kompetenzen bzgl. Verbraucherschutz

- Einführung eines IT-Sicherheits-kennzeichens
- Warnung vor Sicherheitslücken, Schadprogrammen und unerlaubten Datenzugriffen sowie die Empfehlung von Vorkehrungen und Gegenmaßnahmen

Bußgeld

Erhöhung der **Bußgelder:**

- Erhöhung der Bußgeldrahmen bis zu 20 Mio. €
- Erweiterung der Kataloge zu Bußgeldtatbeständen

Anforderungen und Handlungsmöglichkeiten
Gruppe 3: Herstellerpflichten

Herstellerpflichten	Lösungsmöglichkeiten
▪ Verpflichtung von Herstellern von IT-Komponenten ▪ Einsatz von vertrauenswürdigen IT-Komponenten ▪ Für Produkte mit hoher Bedeutung für das Funktionieren des Gemeinwesens ▪ Vertrauenswürdig-keitserklärung über die gesamte Lieferkette ▪ Definition von Mindeststandards durch das BSI	▪ Herstellersicht • Absprache mit den Anwendern um die Fragestellung zu klären • Bereitstellung von vertrauenswürdigen IT-Komponenten ▪ Im Kontext ISO/IEC 27001 ist hier A.15 zu betrachten (Lieferanten- und Dienstleisteraudits) ▪ Prozess zum Monitoring der Anwender etablieren ▪ Dokumentation als Nachweis

Änderungen im IT-SiG
Gruppe 4: Bußgeld

BSI-Befugnisse

Weitere Aufgaben und Kompetenzen z. B.:

- Suche nach Sicherheitslücken
- Detektion von Risiken
- Sammlung von Informationen über Sicherheitsrisiken
- Festlegung von Mindeststandards

Betroffenheit

Weitere **betroffene Unternehmen** inkl. Erweiterung der ihnen auferlegten Pflichten:

- „Entsorgung“
- Infrastrukturen im besonderem öffentlichen Interesse
- Anbieter von Telekommunikations-diensten

Herstellerpflichten

Verpflichtung von **Herstellern** von **IT-Komponenten**

- Für Produkte mit hoher Bedeutung für das Funktionieren des Gemeinwesens
- Vertrauenswürdig-keitserklärung über Lieferkette
- Definition von Mindeststandards durch das BSI

Verbraucherschutz

BSI erhält weitere Kompetenzen bzgl. Verbraucherschutz

- Einführung eines IT-Sicherheits-kennzeichens
- Warnung vor Sicherheitslücken, Schadprogrammen und unerlaubten Datenzugriffen sowie die Empfehlung von Vorkehrungen und Gegenmaßnahmen

Bußgeld

Erhöhung der **Bußgelder:**

- Erhöhung der Bußgeldrahmen bis zu 20 Mio. €
- Erweiterung der Kataloge zu Bußgeldtatbeständen

Anforderungen und Handlungsmöglichkeiten
Gruppe 4: Bußgeld

Bußgeld	Lösungsmöglichkeiten
Erhöhung der **Bußgelder:** ▪ Erhöhung der Bußgeld-rahmen bis zu 20 Mio. € ▪ Erweiterung der Kataloge zu Bußgeldtatbeständen ▪ Kein Straftatbestand (war zunächst geplant)	▪ Frühzeitige Evaluierung der Auswirkungen auf das Unternehmen ▪ Schaffen von Awareness ▪ Einbindung von Unternehmensleitung und Compliance ▪ Transparenz ▪ Abhängigkeiten zu den weiteren Anforderungen

03

Konkrete umzusetzende Anforderungen für Technologie-lieferanten

IT-SiG 2.0
Konkrete umzusetzende Anforderungen

- Einrichtung & Betrieb eines ISMS
- Härtung aller Systeme mit externen Schnittstellen
- Durchführung von Penetration-Tests für Schnittstellen & Systeme
- Ggf. Identifikation & Registrierung
- Selbsterklärung IT-Sicherheit (Behörden, Kunden)
- Vorfallsmeldungen an Steakholder absetzen
- Lieferketten absichern
- Systeme zur Angriffserkennung & Analyse etablieren

IT-SiG 2.0
Empfohlene Anforderungen

- Lieferketten betrachten & nachweisen können
- Systemkomponenten von Produkten aus „vertrauenswürdigen Quellen“ verwenden
- Zertifizierungen für Produkte anstreben
- Anforderungen an KRITIS-Betreiber kennen & unterstützen

IT-SiG 2.0

Häufige Fragen aus der Praxis

Ab wann muss die Garantieerklärung erstmalig vorliegen?

Was versteht der Gesetzgeber unter „Art der kritischen Komponente“?

Wie werden die Betreiber über neue Allgemeinverfügungen etc. zum IT-SiG 2.0 informiert?

Was empfiehlt der Technologielieferant?

Welche Fristen müssen wir einhalten?

Muss die Garantieerklärung auch für die bereits genutzten Systeme eingeholt werden?

IT-SiG 2.0

Häufige Fragen aus der Praxis

Welche Schwellwerte oder Kennzahlen gelten für mich?

Seit wann gilt für mich das IT-SiG 2.0?

Wann kann oder muss ich meine Lieferanten oder Hersteller kontaktieren und abfragen?

Was zählt als kritische Komponente? Geht es um jeden Typ oder um jedes Gerät?

IT-SiG 2.0
Potenzielle Herangehensweise

- Durchführung einer Ist-/Soll-Analyse, z. B. SWOT-Analyse, um den Handlungsbedarf zu identifizieren
- Ausarbeitung eines Action-Plans „IT-SiG 2.0“
- Prüfung und Festlegung, wie die praktische Umsetzung erfolgen kann/soll
- Monitoring der sich entwickelnden Rechtslage (Allgemeinverfügungen zum IT-SiG 2.0 etc.)

04

Heraus-forderungen und Chancen

Neue Herausforderungen, aber auch neue Chancen

Neue Herausforderungen	Neue Chancen
▪ Ganzheitlicher Ansatz, bei welchem die Gesamtheit der vernetzten Komponenten einer Organisation betrachtet werden ▪ Einführung von Systemen und Prozessen zur Erkennung und Behandlung von Angriffen bzw. Angriffsversuchen ▪ Monitoring der Hersteller, ob eine aktuelle Vertrauenswürdigkeitserklärung vorliegt ▪ Monitoring der Zulieferer, ob die Standards des BSI erfüllt und nachgewiesen werden können (z. B. hinsichtlich des Datenschutzes)	▪ Erhöhung der Informationssicherheit bei den KRITIS-Betreibern ▪ Steigerung der Sicherheit für IT-Systeme und digitale Infrastrukturen ▪ Modernisierung und Ausbau der IT-Security-Systeme ▪ Aktualisierung der Prozesse im Rahmen des ISMS ▪ Hersteller und Zulieferer können hinsichtlich ihrer Integrität besser beurteilt werden

Betreiber setzen bereits viele der Anforderungen nach Stand der Technik in der IT-Sicherheit um

CONSULTING	PRODUKTE / LÖSUNGEN
IT-Sicherheitsarchitekturen	Sicheres IIoT Edge Computing u. Connectivity
IT-Sicherheitskonzepte	ICS / OT Netzwerk – Security Monitoring
Informationssicherheitsmanagement (ISMS)	Gekapselte Legacy-Anlagen-Software
Business Continuity Management (BCM)	Sicherheitsgekapselter Internet-Browser
Audit & Revision	Sicherer mobiler Arbeitsplatz
Security Awareness	Multifaktor-Authentifizierung
Sicherheitsanalysen	Public-Key-Infrastruktur (PKI)
Penetrationstests	Sichere Cloud-Infrastruktur-Plattform

Mehr Informationen: secunet.com

Björn Huber-Puls
Senior Berater Informationssicherheit
Management Systems & Audit
Division Industry

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Telefon +49 201 5454-2452
Telefax +49 201 5454-0
bjoern.huber-puls@secunet.com

Frank Hülle
Senior Berater
Management Systems & Audit
Division Industry

secunet Security Networks AG
Konrad-Zuse-Platz 2-4
81829 München
Telefon +49 201 5454-2667
Telefax +49 201 5454-1327
frank.huelle@secunet.com

secunet