Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

ITSiG im Bereich KMU

Stephan Krischke, ProtectYourIT

Agenda

- Teil 1: Das Gesetz und die Unternehmen
- Teil 2: Praxisbeispiel anhand eines kleinen Unternehmens

Teil 1: ITSiG und KMU

Fakten

"Mit der zunehmenden digitalen Durchdringung unseres Lebens wird Cyber-Sicherheit immer mehr zu einem zentralen Baustein der Inneren Sicherheit in unserem Land.

Unser Ziel ist es daher, dass die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit gehören."

Das Gesetz wurde am 12.06.2015 verkündet und trat am 25.07.2015 in Kraft.

Teil 1: ITSiG und KMU

Fakten

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)

Die Anzahl der im Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz genannten bis zu 2 000 Betreiber über alle sieben Sektoren lässt sich gegenwärtig insoweit konkretisieren, als durch diese Verordnung für die vier Sektoren Energie, Wasser, Ernährung und IKT 730 Kritische Infrastrukturen erfasst werden. Eine darüber hinausgehende Konkretisierung kann erfolgen, wenn die noch ausstehenden Sektoren Transport und Verkehr, Gesundheit und Finanz- und Versicherungswesen geregelt werden.

Einstufung von ca. 730 Unternehmen als gemäß Rechtsverordnung Teil 1

Teil 1: ITSiG und KMU

Definition ITSiG

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- Erweiterte Anforderungen für Webseitenbetreiber (TMG)
- Betreiber kritischer Infrastrukturen (KRITIS)
- Ausnahme solcher Unternehmen, die Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG sind

Teil 1: ITSiG und KMU

Definition KMU (Kleine und mittlere Unternehmen)

Größenklasse	Tätige Personen		Jahresumsatz		
KMU					
Kleinstunternehmen	bis 9	*und*	bis 2 Mill. EUR		
Kleine Unternehmen	bis 49	*und*	bis 10 Mill. EUR	*und*	kein Kleinstunternehmen
Mittlere Unternehmen	bis 249	*und*	bis 50 Mill. EUR	*und*	kein kleines Unternehmen
Großunternehmen	über 249	*oder*	über 50 Mill. EUR		

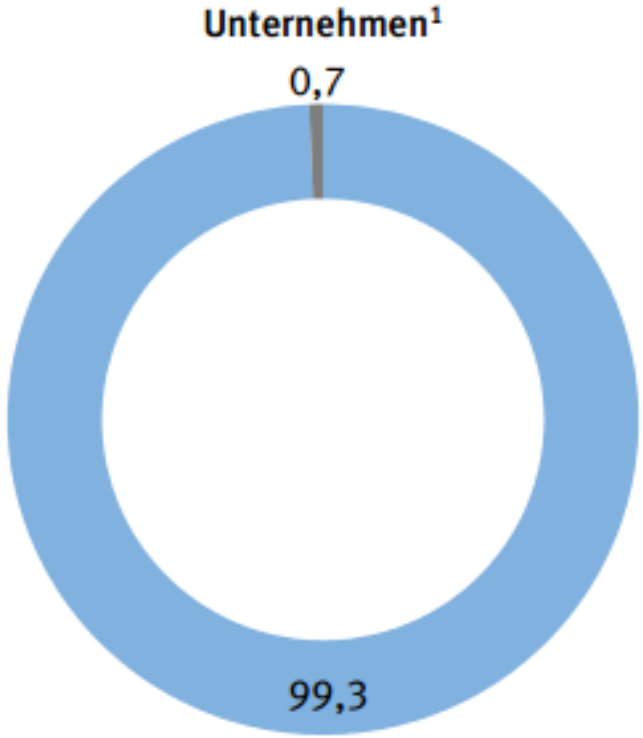
Quelle: Statistisches Bundesamt, Wirtschaft und Statistik, Januar 2014

Übereinstimmung mit Empfehlung 2003/361/EG der Kommission

Teil 1: ITSiG und KMU

Unternehmen 2011

in %



Kleine und mittlere Unternehmen

Großunternehmen

1 Einschließlich abhängiger Unternehmen.

2014 - 01 - 0034

Quelle: Statistisches Bundesamt, Wirtschaft und Statistik, Januar 2014

Teil 1: ITSiG und KMU

8.1 Vorhandene **IT-Sicherheitsrichtlinie** nach Wirtschaftszweigen und Beschäftigtengrößenklassen

Wirtschaftszweig	Unternehmen mit einer formell festgelegten IT-Sicherheitsrichtlinie			
	Insgesamt	Unternehmen mit ... bis ... Beschäftigten		
		10 - 49	50 - 249	250 und mehr
	Anteil in % an den Unternehmen mit Computernutzung (ohne Unternehmen mit 1 bis 9 Beschäftigten)			
Untersuchte Bereiche insgesamt	**29**	**23**	**48**	**73**
Verarbeitendes Gewerbe	31	21	48	77
Energie- und Wasserversorgung, Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen	44	35	57	86
Baugewerbe	/	/	29	66
Handel, Instandhaltung und Reparatur von Kraftfahrzeugen	28	23	48	65
Verkehr, Lagerei, Post-, Kurier- und Expressdienste	20	/	40	73
Gastgewerbe	19	15	41	71
Information und Kommunikation	58	52	77	87
Grundstücks- und Wohnungswesen	47	42	77	100
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen	43	38	76	83
Erbringung von sonstigen wirtschaftlichen Dienstleistungen	26	/	33	60
Reparatur von Datenverarbeitungs- und Telekommunikationsgeräten	/	/	/	/

Quelle: Statistisches Bundesamt, 2015

Teil 1: ITSiG und KMU

Kritik

- Nur ca. 730 Großunternehmen sind KRITIS
- Großunternehmen haben bessere Vorrausetzungen
- KMU hat höheren Bedarf, jedoch noch nicht vom ITSiG betroffen
- Verbesserung der IT-Sicherheit in KMU durch ITSiG fraglich

Agenda

- Teil 1: Das Gesetz und die Unternehmen
- Teil 2: Praxisbeispiel anhand eines kleinen Unternehmens

Teil 2: ISMS in KMU

Beweggründe zur Einführung eines ISMS?

- Als Zulieferer eines Großunternehmens oder Konzerns
- Sicherheitsvorfall

Teil 2: ISMS in KMU

Leitfäden und Best Practices

UP KRITIS

Best-Practice-Empfehlungen

für Anforderungen an Lieferanten

zur Gewährleistung der Informationssicherheit

in Kritischen Infrastrukturen

Version 1.2 vom 05.07.2016

THEMEN | SERVICES | PRESSE | VERBAND | DE | VDA Verband der Automobilindustrie

Publikationen

Information Security Assessment

Sonstiges, 04. März 2015

Überarbeiteter Fragenkatalog „Information Security Assessment“ zur Informationssicherheitsbewertung, Vers. 2.1.3 (22.05.2015), basierend auf der ISO 27002:2013 mit zusätzlichen Controls für die Überprüfung des Information Security Management Systems (ISMS)

Verfügbare Sprachen: Deutsch, Englisch

DOWNLOAD

Teil 2: ISMS in KMU

UP KRITIS

a. Vulnerability-Management (Kapitel 4)
b. Patch-Management (Kapitel 5)
c. Systemhärtung (Kapitel 6)
d. Fernzugang für Drittanbieter (Kapitel 7)
e. Anforderungen an die Softwareentwicklungsprozesse (Kapitel 8)
f. Einsatz der kryptographischen Lösungen (Kapitel 9)
g. Dokumentation (Kapitel 11)
h. Benachrichtigung über sicherheitsrelevante Vorfälle (Kapitel 12)
i. Nicht-technische Sicherheit (Kapitel 13)
j. Informationssicherheitsprozesse / ISMS
k. Zugriffsschutz und Berechtigungsvergabe
l. Asset-Management
m. Personalsicherheit (HR-Security)
n. Physische Sicherheit und Zutrittsschutz
o. Operationelle IS-Anforderungen (Netzwerksicherheit, Virenschutz, Logging & Monitoring, Backup & Restore, etc.)
p. Sicherheit in der Softwareentwicklung und Change-Prozesse
q. Security-Incident-Management
r. Sicherheit in Auslagerungsprozessen

VDA Verband der Automobilindustrie

- Audits
  - Security Assessment
    - Controls
      - 0 VDA Information Security Assessment (DE)
      - 1 General Aspects
      - 5 Information Security Policies
      - 6 Organization of Information Security
      - 7 Human Resources Security
      - 8 Asset Management
      - 9 Access Control
      - 10 Cryptography
      - 11 Physical and Environmental Security
      - 12 Operations Security
      - 13 Communications Security
      - 14 System acquisition, development and maintenance
      - 15 Supplier Relationships
      - 16 Information Security Incident Management
      - 17 Information Security Aspects of Business Continuity Management
      - 18 Compliance

Teil 2: ISMS in KMU

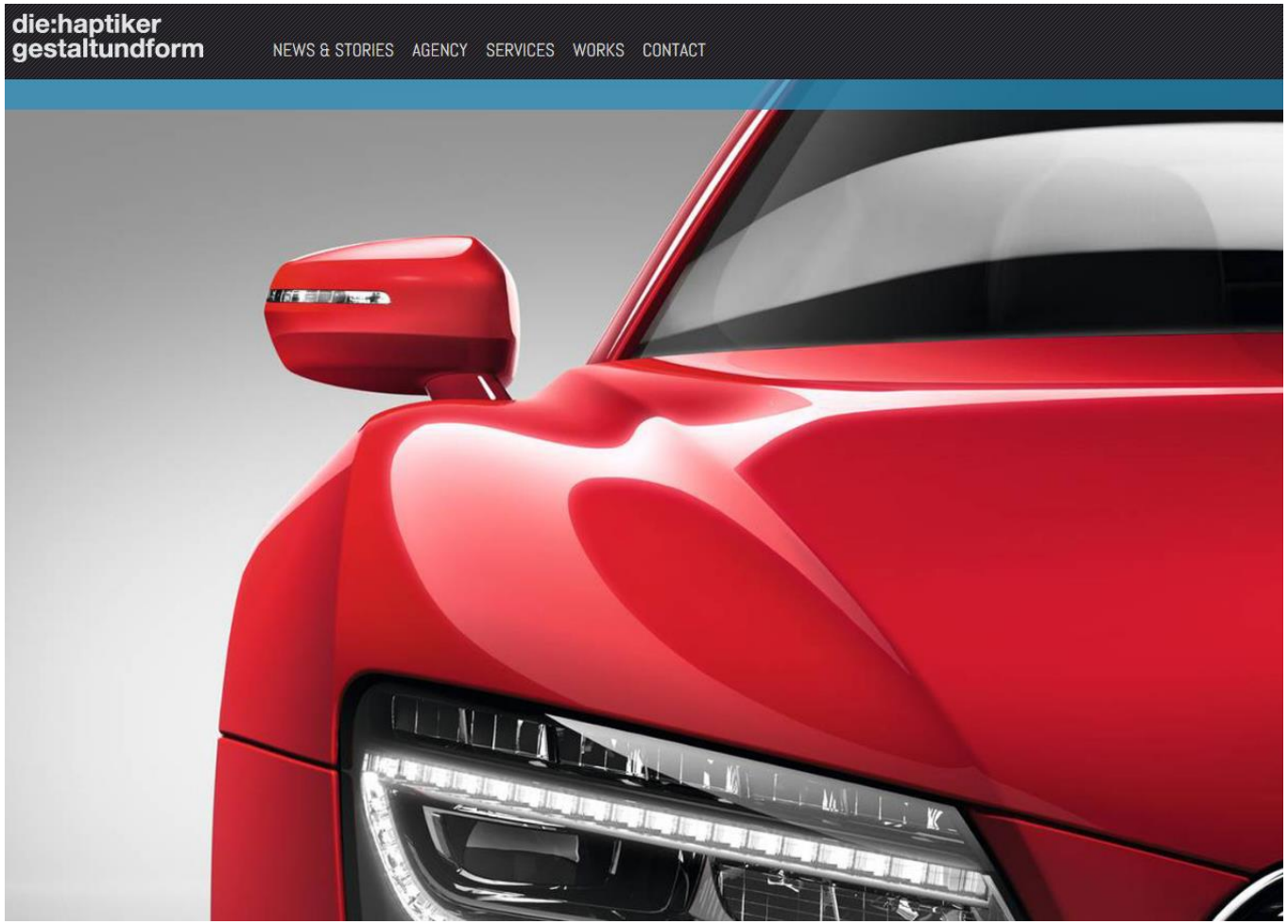
Besonderheiten KMU

- ISMS / Zertifizierung steht nicht im Fokus
- Begrenzte personelle IT Ressourcen
  - ➢Erster Ansprechpartner ist teilweise der IT-Dienstleister
- Kleine finanzielle Budgets
  - ➢Förderungsmöglichkeiten prüfen (bspw. Digital Bonus Bayern)
- Projektverlauf ist "technisch"

Teil 2: ISMS in KMU

Referenzprojekt

- www.die-haptiker.de
- Industriedesign
- 30 Mitarbeiter
- Zulieferer VW/Audi
- ISMS Anforderungen gemäß VDA



Teil 2: ISMS in KMU

Herausforderungen

- ISMS Einführung innerhalb 6 Monate
- IT-Status mit deutlichen Schwachstellen
- Kein ISMS vorhanden
- Keine interne IT vorhanden
- Kleines Projektbudget

Teil 2: ISMS in KMU

Zeitlicher Projektverlauf

- ISMS "Quick-Check" und Festlegung von Sofortmaßnahmen
- Risikobewertung gemäß BSI Standard 100-3 und VDA
- Umsetzung technische und organisatorische Sofortmaßnahmen
- ISMS-Audit durch Kunde gemäß VDA Fragenkatalog ISO 27002
- Beschreibung weiterer Maßnahmen
- Umsetzung technische und organisatorische Maßnahmen
- Ergebnisprüfung und Lieferantenfreigabe durch Kunde

Teil 2: ISMS in KMU

- Bestellung eines internen IT-Sicherheitsbeauftragten
- Arbeitsplattform auf Basis Sharepoint
- Installation zentrale Datenstruktur für IT-(ISMS)Management und Betriebs- / Sicherheitshandbuchs
- Erstellung grundlegende Richtlinien und Vereinbarungen
- Ableitung Prozesse und Dokumente anhand Umsetzung technischer Maßnahmen
- Outsourcing IT Prozesse (Managed IT-Services)
- Schulung Mitarbeiter

Teil 2: ISMS in KMU

Projektschwerpunkte

- Einteilung Sicherheitszonen
- Zugangs- und Zugriffskontrolle
- Datenklassifizierung
- Segmentierung Netzwerk
- Redundanzen innerhalb IT-Infrastruktur
- Mobile Datengeräte
- Verschlüsselung

Teil 2: ISMS im KMU

Fazit

- ISMS Leitfaden/Prüfkatalog gemäß VDA und UP KRITIS ausreichend
- Steigerung des Sicherheitsniveau im KMU gemäß ITSiG
- Erkennbares Wachstum bis 2018
- Pragmatische Vorgehensweise erforderlich
- Zusammenarbeit mit IT-Systemhäusern
- Weitere Anforderungen an KMU durch ITSiG (Webseitenbetreiber)?

BISG Wir fördern IT-Sicherheit

Vielen Dank!

Fragen & Anmerkungen?

www.ProtectYourIT.de

www.bisg-ev.de