Datenschutzmanagement
als
integraler Bestandteil
eines
Informationssicherheitsmanagementsystems (ISMS)

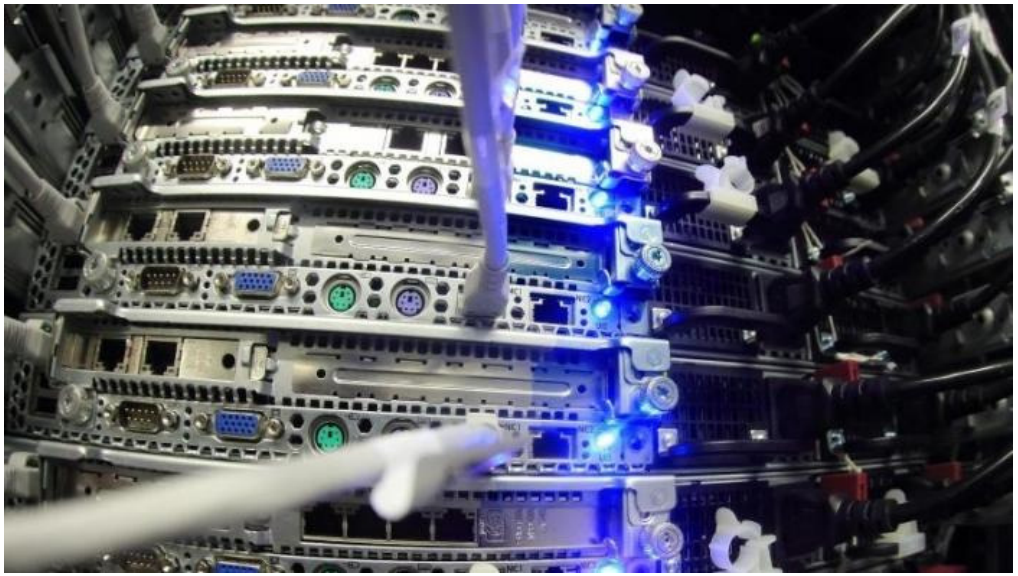
Ein Appell

Stefan Käsler Dipl. Ing. (FH) / Dipl. Wirt. Ing. (FH)
Six Sigma Black Belt, Datenschutzbeauftragter (TÜV), Datenschutzauditor (TÜV), IT-Security Manager (TÜV) , IT-Security Auditor (TÜV) , IT-Compliance Manager (TÜV)

Aktuell zum Einstieg

Branchenindex:
Deutschland bietet weltweit bestes Umfeld für Cloud Computing

06.03.2018 Stefan Krempl (heise)



(Bild: dpa, Jens Wolf)

Die Software-Allianz BSA hat Deutschland rechtlich gesehen zum weltweit besten Standort für Cloud-Dienste vor Japan und den USA erkoren. Die Bundesrepublik punktet in den Bereichen **Datenschutz**, **IT-Sicherheit** und Breitband.

Agenda

- Kurze Vorstellung Stefan Käsler iprosec
- Begriffsklärungen – Informationssicherheit, Datenschutz…
- Die EU-DS-GVO als aktueller Treiber für ein Managementsystem
- Warum sollte der Datenschutz ein integrales Element eines ISMS sein?
- Fazit

Stefan Käsler

Dipl. Ing. (FH) / Dipl. Wirt. Ing. (FH)

- Seit mehr als 25 Jahren Changemanager mit IT Schwerpunkt

- Geschäftsprozessmanager – Six Sigma Black Belt / BPMN
- Projektmanager – IPMA

- Datenschutzbeauftragter (TÜV) und Datenschutzauditor (TÜV)

- IT-Security Manager (TÜV) und IT-Security Auditor (TÜV)
- Zusatzkompetenz §8a BSIG (Kritis), als Prüfer beim BSI gelistet

- IT-Compliance Manager (TÜV)

Disclaimer & Quellenangaben

- Dieser Vortrag betreibt und ersetzt keine Rechtsberatung bezüglich angesprochener Gesetze und Verordnungen.
- Einige Quellen für diesen Vortrag sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) *https://www.bsi.bund.de/, weitere Quellen sind angegeben*
- Gesetzestexte: http://www.gesetze-im-internet.de

Begriffsklärung

Datenschutz
Persönlichkeitsschutz beim Umgang mit personenbezogenen Daten

Aussagen zum Datenschutz:
Der Datenschutz schützt keine Daten sondern Menschen (Betroffene Personen).
Der Schutz der personenbezogenen Daten ist das Ziel des Datenschutz.

Begriffsklärung

Datensicherheit
Technische und organisatorische Maßnahmen zur Sicherung der Programme, Datenbestände und der DV-Anlagen vor
Missbrauch -> Erhalt der **Vertraulichkeit**
Verlust -> Erhalt der **Verfügbarkeit**
Fehlern -> Erhalt der **Integrität**
Identitätsverfälschung - > Erhalt der **Verbindlichkeit**

Begriffsklärung

Compliance (Quelle: Duden)
complere, lateinisch erfüllen – www.complere.de
(Wirtschaftsjargon) regelgerechtes, vorschriftsgemäßes, ethisch korrektes Verhalten

IT-Sicherheit (Quelle: Glossar BSI)
IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.

Informationssicherheit (Quelle: *ISO 27001)*
Informationssicherheit ist die Aufrechterhaltung der Verfügbarkeit, Integrität und der Vertraulichkeit von Informationen.

Begriffsklärung

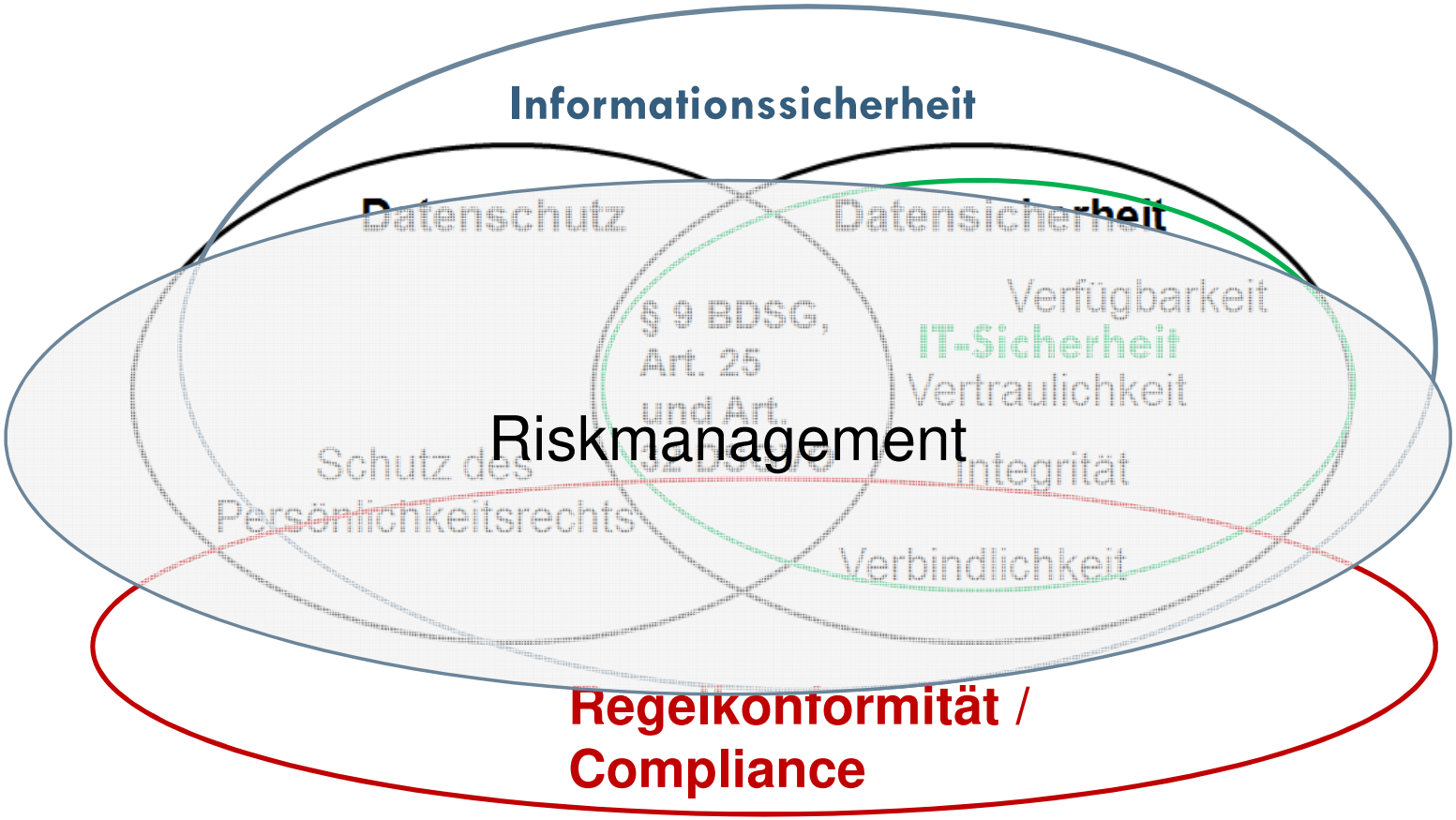
Schutzziele der Informationssicherheit:

Verfügbarkeit = Schutz gegen Verlust

Integrität = Schutz gegen Fehler

Vertraulichkeit = Schutz gegen Missbrauch

Begriffsklärung und Zusammenhänge



Ein Negativbeispiel für sehr starre Kompetenzbereiche

Ein deutscher Großkonzern hatte den Bußgeldbescheid eines Landesdatenschutzbeauftragten akzeptiert und zahlte das verhängte Bußgeld in Höhe von über einer Millionen Euro.

Mit dem Bußgeldbescheid wurden alle bekannt gewordenen Datenschutzverstöße bei diesem Unternehmen geahndet, soweit sie nicht schon verjährt waren. Dabei ging es vor allem um mehrere "Rasterfahndungen" in den Jahren 2002 bis 2005, bei denen ohne konkreten Anlass zur Korruptionsbekämpfung heimlich die Daten einer großen Zahl von Mitarbeitern und deren Angehörigen mit denen von Lieferanten abgeglichen wurden.

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO:

- seit **24. Mai 2016** in Kraft
- anwendbar ab dem **25. Mai 2018**
- **unmittelbar wirksam**
- das aktuelle BDSG ist ab dem 25. Mai ungültig

in 9 Wochen!

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO was ist **nicht** neu**:**

- viele Paragraphen und Regelungen aus dem BDSG finden sich – leicht verändert – in der DS-GVO und im BDSG (neu) wieder
- durch Öffnungsklauseln bleiben, wie u.a. die deutschen Regelungen zum betr. DSB erhalten
- Technische und Organisatorische Maßnahmen (TOM) kennt auch schon das alte BDSG

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO was ist neu – hier nur wenige Punkte!:

- Das Haftungsrisiko steigt extrem (Bußgelder: 66,7 bis 120 fach).
- Art. 5 (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).
- Art. 32 Sicherheit der Verarbeitung

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO Art. 32 Sicherheit der Verarbeitung:

(1) Unter Berücksichtigung **des Stands der Technik**, der **Implementierungskosten** und der **Art, des Umfangs, der Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO Art. 32 Sicherheit der Verarbeitung:

diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, **die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer** sicherzustellen;
- die Fähigkeit, **die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen** bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die EU-DS-GVO als aktueller Treiber für ein Managementsystem

DS-GVO Art. 32 Sicherheit der Verarbeitung:

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere **die Risiken zu berücksichtigen**, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Warum sollte der Datenschutz ein integrales Element eines ISMS sein?

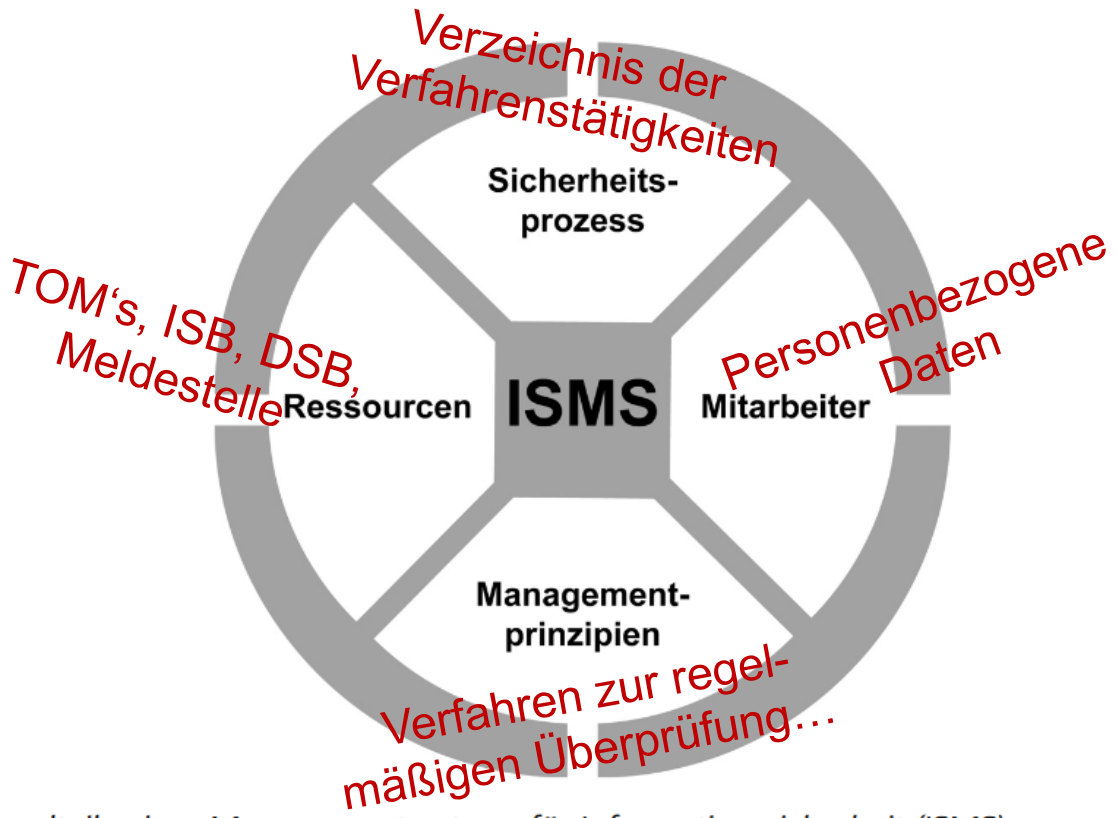


Abbildung 2: Bestandteile eines Managementsystems für Informationssicherheit (ISMS) Quelle: BSI-Standard 200-1

Warum sollte der Datenschutz ein integrales Element eines ISMS sein?

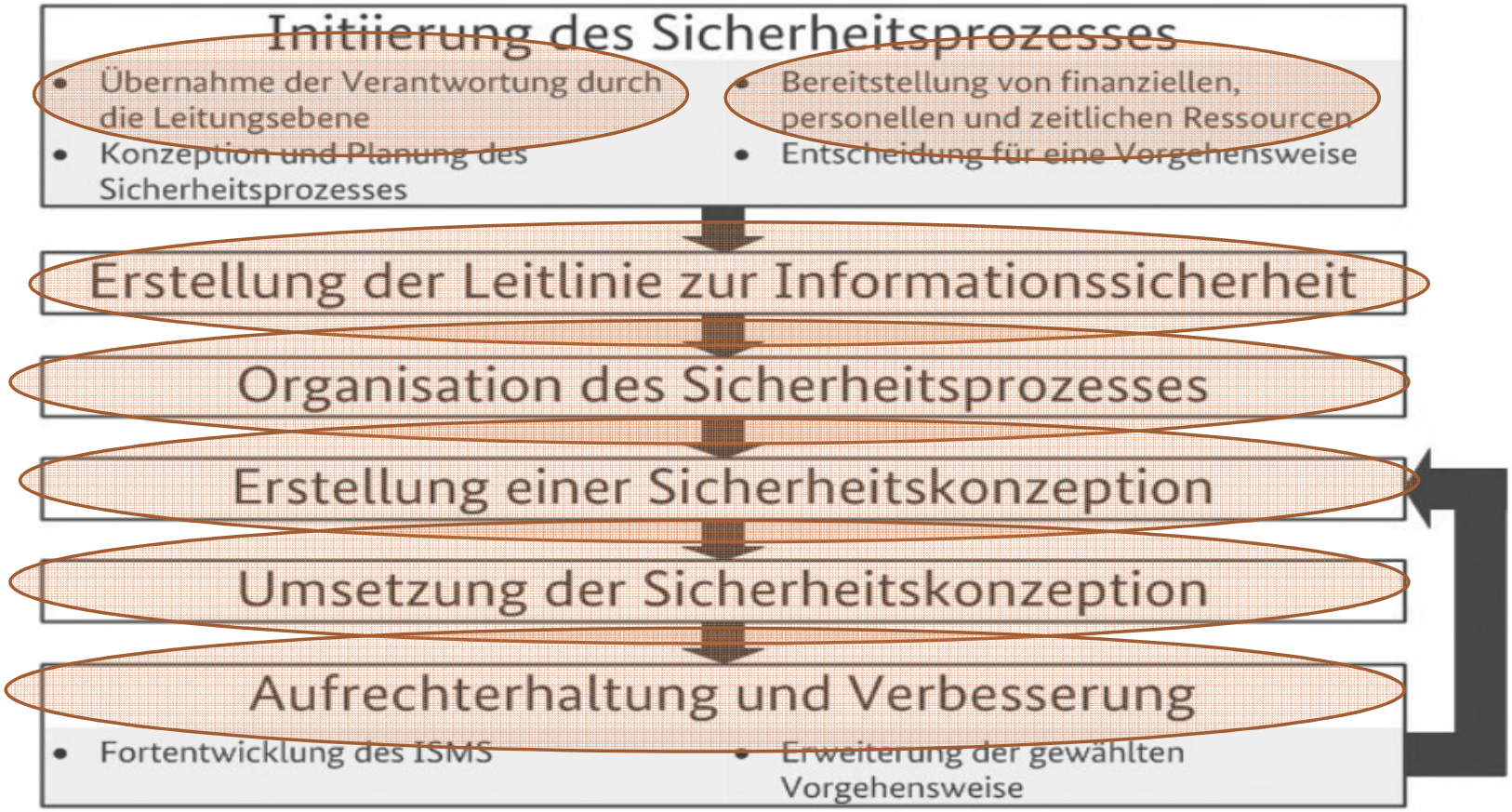


Abbildung 1: Phasen des Sicherheitsprozesses

Warum sollte der Datenschutz ein integrales Element eines ISMS sein?

- Es gibt kaum einen Geschäftsprozess in dem keine personenbezogenen oder personenbeziehbaren Daten verarbeitet werden.
- Die zu schützenden Prozesse (Informationen) sind aus informationstechnischer Unternehmenssicht oft die gleichen, wie die, der betroffenen Personen
- Die Systeme und Netze auf denen die Daten verarbeitet werden sind ebenfalls die gleichen.
- Die Planer, Projektmitglieder, Administratoren und Anwender sind Menschen / betroffene Personen mit Schwächen, eigenen Vorstellungen und Ansprüchen.

Warum sollte der Datenschutz ein integrales Element eines ISMS sein?

- Durch eine frühzeitig parallelisierte Bearbeitung der Anforderungen werden Ressourcen optimal eingesetzt - Zeit und Geld gespart.
- Einbeziehung von Informationssicherheits- und Datenschutzaspekten zu einem sehr frühen Zeitpunkt der Projektplanung erspart unerwartete Zeitverzögerungen und/oder Kostenexplosionen.
- Die Integration von Datenschutzmanagement in ein ISMS schafft Wettbewerbsvorteile gerade in Anbetracht der Unsicherheiten, die sich auch aus der DS-GVO ergeben.
- Ein DSMS reicht in der Regel nicht immer aus, da es entweder neben einem ISMS betrieben wird, oder wichtige gesetzliche Aspekte vernachlässigen könnte.
- Es gibt Unterstützungsmöglichkeiten / Software, die beide Aspekte gleichermaßen berücksichtigt, Synergien schafft und Ressourcen schonen kann.

Warum sollte der Datenschutz ein integrales Element eines ISMS sein?

Wichtig:

In der Organisation muss die Fachkompetenz für Informationssicherheit und für Datenschutz gleichermaßen existieren oder eingekauft werden!

Fazit:

- öffnen Sie Ihre „Burgen“
- schauen Sie über den „Tellerrand“ und informieren und interessieren Sie sich für die Themen des jeweils Anderen
- versetzen Sie sich in den Standpunkt des Kollegen
- arbeiten Sie möglichst schon frühzeitig zusammen
- informieren Sie die Verantwortlichen über Sinn und Zweck der Zusammenarbeit
- haben Sie keine Angst in der Zukunft nicht mehr genug Aufgaben zu haben – die gehen nicht aus!
- Software ist zunächst einmal nur Mittel zum Zweck.
  Sie kann die Bearbeitung aber erheblich rationalisieren, vor allem wenn in ihr Datenschutz und Informationssicherheit gleichermaßen und übergreifend behandelt werden kann, wie in **verinice**!

Gerne stehe ich Ihnen für weitere Fragen zur Verfügung?

Stefan Käsler

Goethestraße 75

58566 Kierspe

Telefon: +49 2359 291420

Email: Stefan.Kaesler@iprosec.de