

The top of security.



KRITIS-Dachgesetz

Vorsprung durch Vorbereitung

Warum smarte Unternehmen bereits heute KRITIS ready sind.

Inhalt

02

Vorwort:
Einleitung

04

KRITIS-Dachgesetz und NIS2 - Was Sie jetzt als
Betreiber wissen müssen

06

Betroffene Sektoren und
Anforderungen an die Betreiber

08

Pflichten auf einen Blick - Fristen, Risiken, Chancen

09

Praxislösung PYLOCX® –
Compliance ohne Mehraufwand

15

Fazit und Ausblick

Vorwort

„Das KRITIS-Dachgesetz kommt – Unternehmen und Betreiber stehen somit stärker denn je in der Verantwortung, ihre Systeme vor Ausfällen, Angriffen und Sabotage umfassend zu schützen – digital wie physisch.“



Phillip Schickenberg

Bereichsleiter Vertrieb,
STUV GmbH

Die Sicherheit der Netze und Anlagen ist für Betreiber kritischer Infrastrukturen immer schon eine Aufgabe von zentraler und strategischer Wichtigkeit gewesen.

Als führender Anbieter innovativer und hochsicherer Zutrittslösungen sehen wir es bei Steinbach & Vollmann (STUV) als unsere Aufgabe, Ihnen Orientierung zu den neuen regulatorischen Anforderungen zu geben sowie Lösungsansätze und Handlungspläne zur Verfügung zu stellen, mit denen Sie für die Einführung des KRITIS-Dachgesetzes gewappnet sind.

Einleitung

Ab Inkrafttreten des KRITIS-Dachgesetzes (KRITIS-DG) und des NIS2-Umsetzungsgesetzes drohen Betreibern hohe Bußgelder und persönliches Haftungsrisiko der Geschäftsleitung, wenn Anforderungen nicht fristgerecht umgesetzt werden.

Das zwingt Betreiber schon heute dazu, sich in Bezug auf physische und digitale Sicherheit noch stärker aufzustellen.

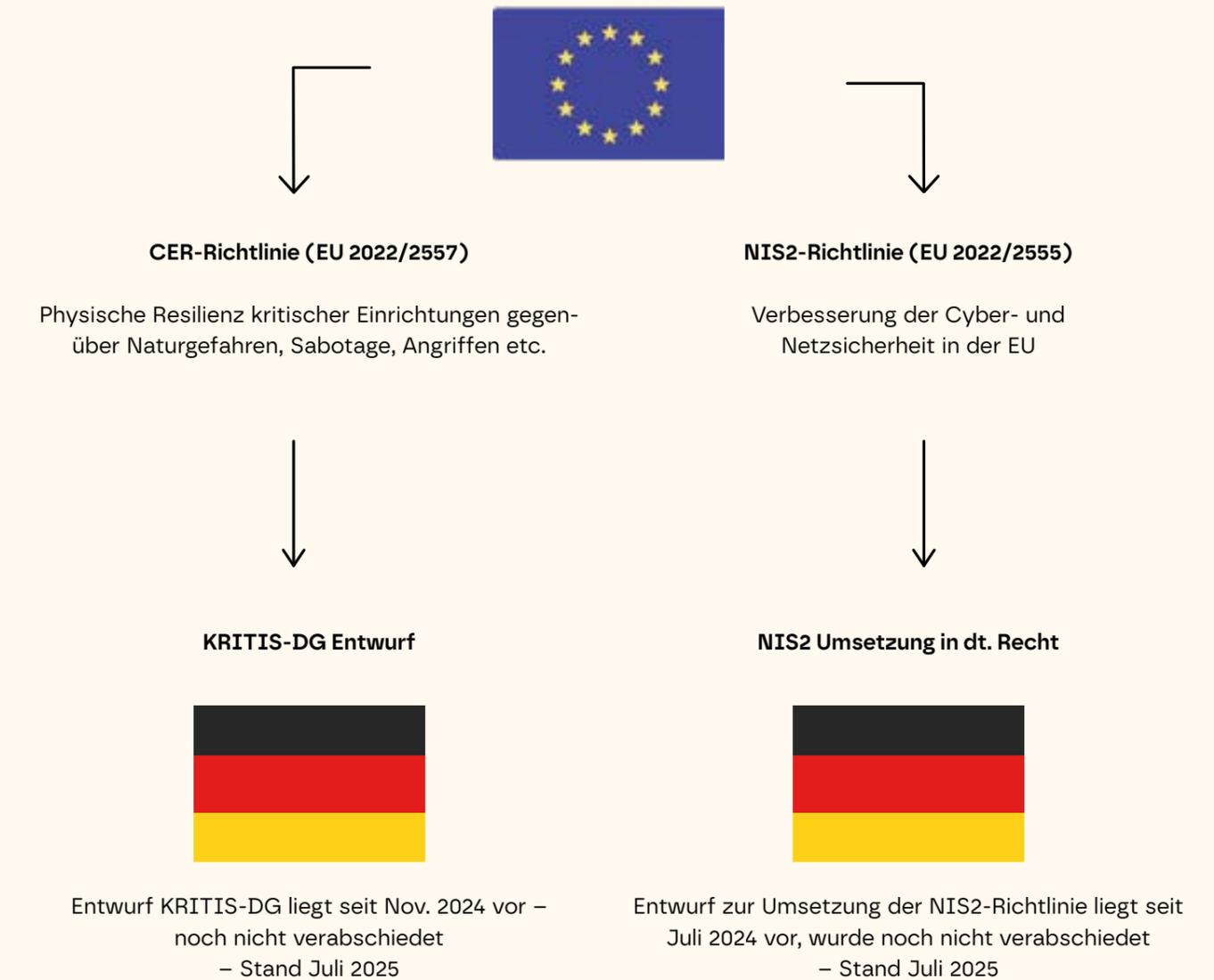
Zugangskontrolle wird zur Schnittstelle zwischen physischer Sicherheit, Datenschutz und betrieblicher Resilienz.



Gesetzliche Ausgangslage

Aktuell hören wir in der öffentlichen Debatte von einer Vielzahl an Begriffen, Namen, Richtlinien und Gesetzesentwürfen.

Hier im Überblick alle relevanten Begriffsdefinitionen:

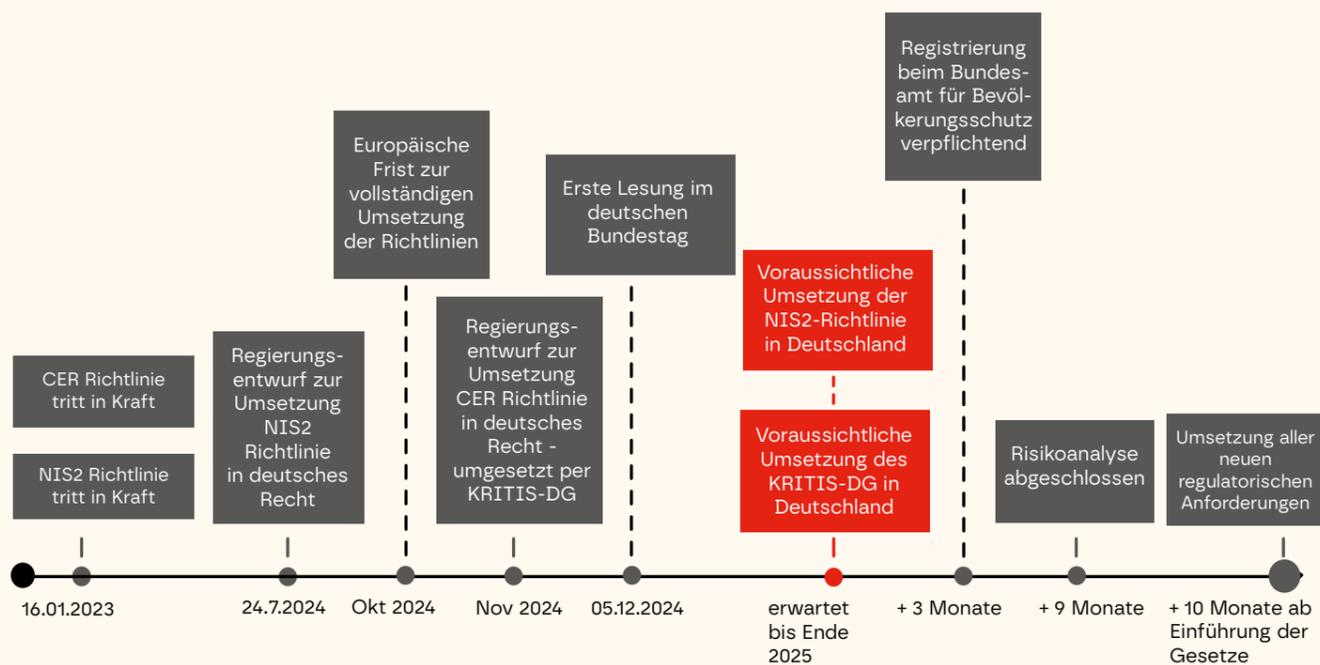


Pflicht zur Umsetzung: Diese Fristen gelten

Mit Stand Juli 2025 haben sieben europäische Länder sowohl die NIS2-Richtlinie (EU 2022/2555) als auch die CER-Richtlinie (EU 2022/2557) vollständig in nationales Recht umgesetzt.

Die Bundesregierung hat im November 2024 das KRITIS-Dachgesetz zur Umsetzung der CER-Richtlinie beschlossen, befindet sich jedoch aktuell noch im parlamentarischen Prozess.

Eine Entscheidung und die Überführung in deutsches Recht wird noch in 2025 erwartet. (Stand Juli 2025)



Die Umsetzungsgesetze europäischen Rechts, NIS2 und das KRITIS-Dachgesetz, verpflichten Betreiber kritischer Infrastrukturen zu umfangreichen Sicherheitsmaßnahmen.

Das Problem: Die Fristen sind kurz, die Anforderungen sind komplex – und die Bußgelder bei Verstößen werden erheblich sein.

Das Ziel: Betreiber müssen digitale und physische Resilienz nachweisen – inklusive Zutrittskontrolle, Notfallpläne und Risikoanalysen.

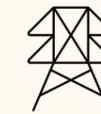
Wer ist betroffen und wann müssen Sie handeln?

Das KRITIS-Dachgesetz betrifft nicht nur Energieversorger.

Jede Organisation, die mit ihrer Dienstleistung das Funktionieren von Wirtschaft, Staat oder Gesellschaft absichert, muss handeln – unabhängig von Größe oder Branche, sofern die definierten Schwellenwerte erreicht werden.

Versorgung & Infrastruktur

- Energieversorger
- Trinkwasserversorgung
- Abfallentsorgung



Risiko: Ausfälle führen zu Versorgungsnotstand und massiven Bußgeldern.

Transport & Verkehr

- Logistik- und Schienenverkehrssektor
- Luft- und Straßenverkehr



Risiko: Unterbrechungen verursachen Lieferkettenausfälle, finanzielle Verluste und Imageschäden.

Gesellschaft & Kommunikation

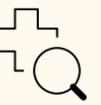
- IT & Telekommunikation
- Medien & Kultur
- Staat & Verwaltung



Risiko: Angriffe gefährden Datensicherheit, Krisenmanagement und öffentliche Ordnung.

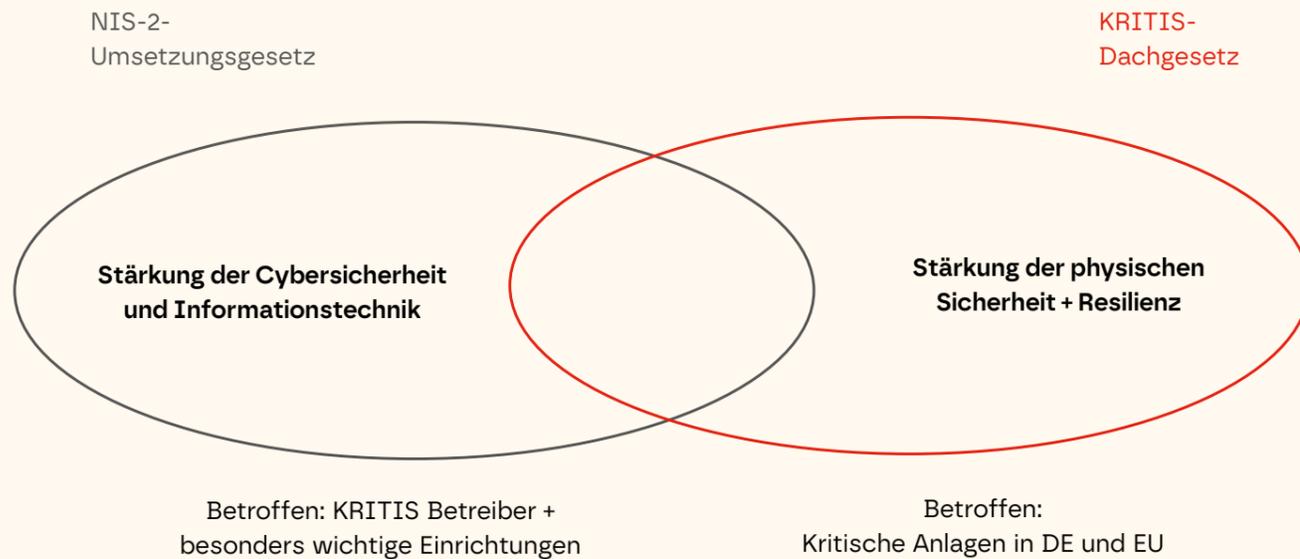
Gesundheit & Wirtschaft

- Krankenhäuser, Labore, Arzneimittel
- Ernährung
- Finanz- und Versicherungswesen



Risiko: Die medizinische Versorgung ist nicht mehr sichergestellt, wirtschaftliche Stabilität ist nicht gewährleistet.

Anforderung an Betreiber



Das KRITIS-Dachgesetz und das NIS2-Umsetzungsgesetz richten sich an Organisationen – einschließlich Unternehmen, Zulieferer und Einrichtungen –, die mit ihren Dienstleistungen eine wesentliche Rolle für das Funktionieren der Gesellschaft und Wirtschaft in Deutschland spielen. Dabei ergänzen sich beide Regelwerke und fokussieren auf unterschiedliche Sicherheitsdimensionen: physische und digitale Sicherheit.

Vorläufige Fristen nach Verabschiedung des KRITIS-DG

- 3 Monate
Registrierung beim Bundesamt für
Bevölkerungsschutz und
Katastrophenhilfe
- 9 Monate
Risikoanalyse und -bewertung
(diese ist alle 4 Jahre zu wiederholen)
- 10 Monate
Aufstellen eines Resilienzplans (tech-
nische, sicherheitsbezogene und
organisatorische Maßnahmen), Ein-
richten eines Meldewesens und Im-
plementierung der Pflichten auf Ge-
schäftsleitungsebene

Was Sie jetzt konkret tun müssen:

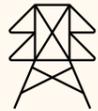
- Registrierung beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- Resilienzplan – physischer Schutz, Abwehr und Folgenbegrenzung, branchenspezifische Resilienzstandards.
- Dokumentation & Meldewesen – Vorfallmeldungen, Reaktion und Abwehr von Vorfällen sowie Folgenbegrenzung.
- Sicherheitsmanagement für eigenes und externes Personal, Schulungen, Übungen, Sensibilisierung.

So erfüllen Sie die KRITIS-Pflichten ohne teure Systemwechsel

Betreiber kritischer Infrastrukturen müssen nach dem KRITIS-Dachgesetz ihre Zutrittssysteme gezielt auf Resilienz, Nachvollziehbarkeit und Schutz vor Ausfällen ausrichten.

Problem: Viele Betreiber setzen noch auf veraltete Systeme, die in Prüfungen nicht mehr akzeptiert werden.

Lösung: Systeme wie PYLOCX® erfüllen heute schon die künftigen Standards – manipulationssicher, retrofit-fähig, ausfallsicher.



Resilienzpflcht

Zukünftige Sicherheitslösungen sollten auch im Blackout-, Krisenfall oder bei Naturkatastrophen funktionieren, wenn Internet- und Mobilfunknetze ausfallen.



Cybersicherheit

Cyberangriffe wie Hacking, Malware oder DDoS-Attacken stören oder blockieren Netzwerke und Systeme. Die Angriffsfläche für Cyberattacken so gering wie möglich zu halten, ist die Aufgabe von Risikoanalysen und der Identifikation kritischer Assets.



Absicherung gegen physische Einwirkung

Gerade im Hinblick auf die steigende Bedrohung durch Sabotage, unbefugten Zutritt und wechselndes Personal ist ein verlässlicher physischer Schutz unerlässlich. In abgelegenen Stationen, Schachtanlagen oder Umspannwerken sind klassische Schließsysteme oft Angriffspunkt Nr. 1.

Mit KRITIS können wir umgehen

PYLOCX® das smarte Zutrittskontrollsystem

PYLOCX® ist ein VdS-zertifiziertes Sicherheitssystem und wurde in Zusammenarbeit mit dem BSI (Bundesamt für Sicherheit in der Informationstechnik) für den Einsatz in der kritischen Infrastruktur entwickelt.

Erfüllt höchste

Sicherheitsanforderungen

- Sicherheit und Schutz vor Cyberangriffen
- VdS-zertifiziertes Schließsystem und mit dem BSI entwickelter Verschlüsselungsalgorithmus
- 100% DSGVO konform, volle Datenkontrolle

Resistent und langlebig

- Extrem vandalismussicher
- Temperatur- und wetterresistent
- Langlebig dank hochwertiger Edelstahlkonstruktion

Schwarzfallsicher

- Keine Stromversorgung im Schloss notwendig
- Offline und autark – PYLOCX® arbeitet auch dann noch, wenn Handy oder Stromnetz ausfallen
- Funktioniert ohne Strom, ohne App und ohne Netzwerkverbindung zum Access Server

Flexibel und modular

- Retrofit-kompatibel
- Customized Lösungen
- Mieten statt kaufen
- Transparente Kostenstruktur

Maßgeschneiderte Sicherheitslösungen

Das smarte PYLOCX® Zutrittskontrollsystem bietet branchenübergreifenden Schutz und ist extra für die kritische Infrastruktur entwickelt – flexibel, effizient und zukunftssicher.



PYLOCX®
Schließzylinder



PYLOCX®
Schwenkhebel-
schloss



PYLOCX®
Elektronikbeschlag



PYLOCX®
Schlüsseldepot



PYLOCX®
Containerschloss



PYLOCX®
Motorschloss



PYGUARD



PYLOCX®
Vorhangschloss

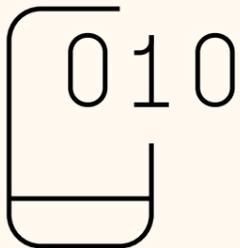
Dank der kompletten Retrofit-Fähigkeit lassen sich unsere Systeme nahtlos in bestehende RFID-Kartensysteme integrieren – Ihre gewohnte Softwareumgebung bleibt vollständig erhalten. Ideal für Unternehmen, die auf nachhaltige Sicherheit ohne Systemwechsel setzen.

So funktioniert PYLOCX®

Das PYLOCX® System kombiniert die Vorteile elektronischer Schließtechnik mit der Robustheit physischer Zugangskontrollen. Der Zugang erfolgt über sichere, manipulationssichere Einmalcodes mit einem flexiblen Berechtigungsmanagement. Eine lückenlose Dokumentation der Zugänge ist jederzeit gewährleistet.



In der Management-Software für das PYLOCX®-Zutrittskontrollsystem werden Nutzer oder Nutzergruppen angelegt. Jedem PYKEY® ist genau 1 Nutzer und 1 PYLOCX®-Schloss zugeordnet. Ein Algorithmus generiert die Einmalcodes.



Der Nutzer erhält Einmalcodes telefonisch, persönlich oder per SMS.

Öffnen und Schließen ganz einfach



Code eingeben

Der Nutzer gibt dann den 8-10 stelligen Einmalcode ein, der zuvor über einen geheimen Algorithmus aus 1: 10 Milliarden Kombinationen generiert wurde.



PYKEY® aufsetzen

Der Nutzer setzt den magnetischen PYKEY® auf die Kontaktstelle aus robustem Edelstahl.



Öffnen

Der Nutzer öffnet das Schloss.



Schließen

Der Nutzer kann das Schloss danach ohne weitere Eingabe von Codes einfach und schnell wieder schließen.

Case Study

Sichere Wasserversorgung dank PYLOCX®

Herausforderung:

Ein großer Wasserversorger in Deutschland sah sich mit steigenden regulatorischen Anforderungen durch das kommende KRITIS-Dachgesetz konfrontiert.

- Schachtanlagen waren unzureichend gesichert
- Das Schlüsselmanagement ist teuer und unsicher

Lösung:

STUV entwickelte eine maßgeschneiderte Lösung mit dem PYLOCX® Schließsystem:

- Integration im bestehenden Schachtdeckel
- Kein Umbau notwendig

Ergebnis:

- 100% KRITIS-konforme Absicherung der Wasserversorgung
- Vermeidung von Sabotage- und Manipulationsrisiken
- Nachrüstung bestehender Infrastruktur ohne Zusatzkosten für Verkabelung
- Kein Schlüsselmanagement Aufwand mehr
- Automatisierte Zutrittskontrolle für Servicetechniker



Case Study

Maximale Sicherheit für Energieversorger

Herausforderung:

Energieversorger sind besonders anfällig für Sabotageakte, Diebstahl und Cyberangriffe. Ein großer Netzbetreiber suchte eine Lösung, um Schaltanlagen, Trafostationen und Außenstationen besser zu schützen.

Lösung:

Mit PYLOCX® konnte der Energieversorger seine Anlagen sichern.

- Schlüsselloses Zutrittsmanagement
- Die Verwaltung erfolgt über eine zentrale Software, die alle Berechtigungen in Echtzeit verwaltet

Ergebnis:

- 100% manipulations-sicherer Zugang zu kritischen Anlagen
- Funktionsfähig auch im Blackout Fall
- Keine Kosten mehr für Schlüsselverwaltung
- Maximaler Schutz gegen Social Engineering und Insider-Bedrohungen
- Cyberresistente Zutrittslösung, die DSGVO- und KRITIS-konform ist



Fazit

Auch wenn das KRITIS-Dachgesetz und das NIS2-Umsetzungsgesetz noch nicht in Kraft sind (Stand Juli 2025), sollten Betreiber kritischer Infrastrukturen keine Zeit verlieren: Die Anforderungen sind absehbar – und die Fristen zur Umsetzung nach Inkrafttreten werden knapp bemessen sein. Es existieren bereits konkrete Empfehlungen und Handlungsrahmen von Institutionen wie dem BSI, dem Bundesministerium des Innern (BMI) sowie Fachverbänden wie BDEW oder DVGW.

Unternehmen, die in puncto Sicherheit vorausplanen, sichern nicht nur Compliance, sondern verschaffen sich einen Wettbewerbsvorteil.

Wer heute handelt, kann spätere Aufwände, Risiken und potenzielle Bußgelder vermeiden.

Gerade im Bereich der physischen Sicherheit liefert das PYLOCX®-System eine zukunftssichere Lösung: DSGVO-konform, manipulationssicher und VdS-geprüft.

Damit erfüllt es schon jetzt zentrale Anforderungen, wie sie sich aus den künftigen gesetzlichen Regelungen ableiten lassen – und bietet damit einen echten Sicherheitsvorsprung.



Ausblick

Sie möchten wissen, was Sie in Fragen der Sicherheit verbessern können?

In nur 30 Minuten erfahren Sie, wie sicher Ihre Infrastruktur wirklich ist

- Check Status quo
- Prüfung aller geplanten Zutrittssituationen
- Identifizierung möglicher Sicherheitsdefizite
- Gap-Definition mit bestehenden Richtlinien
- Handlungsempfehlungen, um Lücken zu schließen

Ihr Kontakt zu STUV

T+49 2056 14 - 0
sales@stuv.info
www.stuv.info

Wir freuen uns darauf,
 Sie kennenzulernen.





Steinbach & Vollmann GmbH

Parkstraße 11
42579 Heiligenhaus
Germany

T +49 2056 -14 0
E sales@stuv.info
www.stuv.info