Beschluss des EK ZÜS **ZÜS B-002 rev 3**

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	16.11.2022
	36. Sitzung, TOP 8.10	15.11.2023
	37. Sitzung, TOP 5.2	17.04.2024

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß § 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

Hinweis: Um den sich ständig ändernden Bedrohungen fortlaufend zu begegnen, ist es für die Cybersicherheit wesentlich, dass diesbezüglich Strukturen und Prozesse eingerichtet und aufrechterhalten werden.

(2) In diesem Beschluss wird der Begriff „Betreiber“ verwendet.

(3) Dieser Beschluss bezieht sich ausschließlich auf Prüfungen, die der Bestätigung der Einhaltung der Vorgaben der BetrSichV dienen. Aspekte, die der Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. personenbezogene Daten) dienen, werden nicht berücksichtigt.

(4) Der Prüfumfang umfasst auch über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile der überwachungsbedürftigen Anlagen (z. B. Notrufeinrichtungen, Alarmierungseinrichtungen) oder andere technische Infrastrukturen, wenn für sie als Ergebnis der Gefährdungsbeurteilung ein Schutz gegen Cyberbedrohungen als erforderlich angesehen wird. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(5) CS-Maßnahmen derjenigen IT/OT[1]-Systeme, die mit schutzbedürftigen Einrichtungen in Verbindung stehen und als Angriffswege genutzt werden können, sind Bestandteil des Prüfumfanges.

[1] OT = Operational Technology

(6) Die Beherrschung von Cyberbedrohungen setzt grundsätzlich auf einen lebenszyklusbegleitenden Prozess zur Cybersicherheit auf.

(7) Die Cybersicherheit ist Gegenstand folgender Prüfungen:

- Anhang 2 Abschnitt 2 Nummern 3 und 4.1 BetrSichV Aufzugsanlagen
- Anhang 2 Abschnitt 3 Nummern 4.1 und 5.1 BetrSichV Explosionssicherheit
- Nach Anhang 2 Abschnitt 4 Nummern 4 und 5 BetrSichV (Prüfung vor Inbetriebnahme von Druckanlagen und wiederkehrende Anlagenprüfungen)
- Prüfbericht zur Erlaubnis nach § 18 Absatz 3 BetrSichV

(8) Schutzbedürftige Einrichtungen, die aufgrund nicht vorhandener Datenschnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können, benötigen keine Maßnahmen der Cybersicherheit.

2 Rechtliche Rahmenbedingungen

(1) Der Betreiber hat gemäß §§ 15 und 16 BetrSichV sicherzustellen, dass überwachungsbedürftige Anlagen vor Inbetriebnahme, vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung und wiederkehrend geprüft werden. Der Betreiber ist gemäß § 3 BetrSichV verpflichtet, Gefährdungen (auch die durch Cyberbedrohungen) zu beurteilen und geeignete Schutzmaßnahmen zu treffen.

(2) Die TRBS 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung, Festlegung und Prüfung erforderlicher CS-Maßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung von Arbeitsmitteln inklusive überwachungsbedürftigen Anlagen eingesetzt werden.

(3) Für die Bereitstellung von Arbeitsmitteln auf dem Markt[2] (Inverkehrbringen) gibt es noch keine verbindlichen Vorgaben zur Cybersicherheit. Deshalb sind die erforderlichen CS-Maßnahmen in der Gefährdungsbeurteilung insbesondere unter Beachtung der Anforderungen der Betriebssicherheitsverordnung, zu ermitteln.

(4) Gemäß § 3 Absatz 2 Satz 2 Nr. 4 BetrSichV muss der Betreiber bei seiner Gefährdungsbeurteilung auch vorhersehbare Betriebsstörungen berücksichtigen.

In TRBS 1111 Abschnitt 4.5 sind vorhersehbare Betriebsstörungen, wie z. B. „Ereignisse, die den Arbeitsablauf behindern oder zur Einstellung der Arbeiten führen oder bei denen die für den Normalbetrieb des Arbeitsmittels getroffenen Schutzmaßnahmen teilweise oder ganz außer Kraft gesetzt sein können“, benannt. Eine solche Betriebsstörung kann auch der plötzliche Ausfall von Sicherheitsfunktionen eines Arbeitsmittels durch Fremdeinwirkung sein. Die möglichen Auswirkungen einer Kompromittierung von schutzbedürftigen OT-Einrichtungen sind daher in der Gefährdungsbeurteilung zu bewerten.

Hinweis: Ergibt sich aus der Gefährdungsbeurteilung, dass ein auf dem Markt bereit gestelltes Arbeitsmittel unter Berücksichtigung der innerbetrieblichen Einsatzbedingungen und der auszuführenden Arbeiten nicht ohne zusätzliche Schutzmaßnahmen sicher verwendet werden kann, hat der Betreiber gemäß § 5 Absatz 1 BetrSichV geeignete Schutzmaßnahmen festzulegen.

[2] Redaktionsschluss März 2024

3 Begriffsbestimmungen im Sinne dieses Beschlusses

(1) Es gelten die Definitionen TRBS 1115-1 für:

- Cybersicherheit,
- Cyberbedrohung,
- IT/OT-Umgebung und
- CS-Maßnahmen

(2) **Schutzbedürftige Einrichtungen** sind:

- Sicherheitsrelevante MSR-Einrichtungen,
- nicht sicherheitsrelevante MSR-Einrichtungen (z. B. PLT-Betriebseinrichtungen), bei denen durch die Kompromittierung ihrer Funktion auch unter Berücksichtigung von Wechselwirkungen mit anderen Anlagenteilen eine relevante Gefährdung von Beschäftigten und anderen Personen im Gefahrenbereich verursacht werden kann
- sicherheitsrelevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen), im Folgenden autarke Sicherheitseinrichtungen genannt,

soweit eine Kompromittierung durch Cyberbedrohungen möglich ist. Sowie

- Teile der IT/OT-Umgebung für die CS-Maßnahmen zum Schutz von Angriffszielen erforderlich sind.

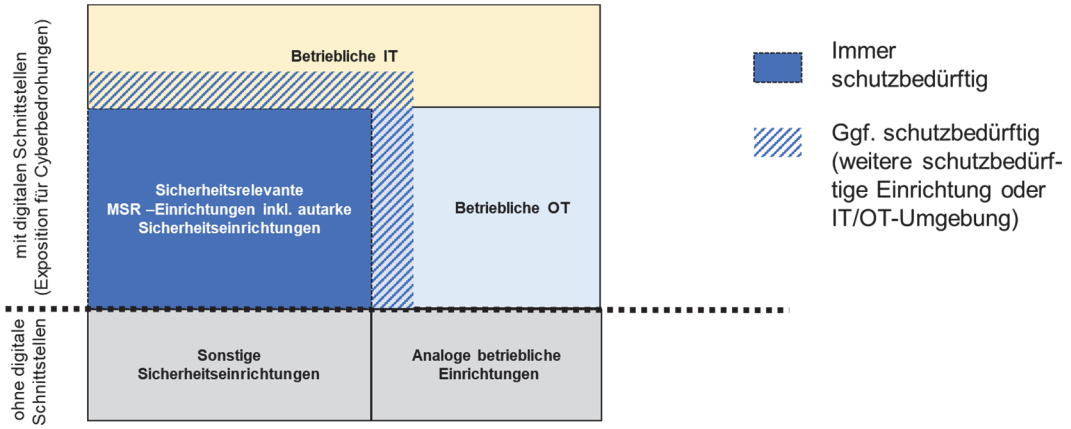

Abbildung 1: Darstellung der schutzbedürftigen Einrichtungen und der IT/OT-Umgebung

4 Prüfung der CS-Maßnahmen für schutzbedürftige Einrichtungen

Vorbemerkung:

Die folgenden Prüfschritte richten sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der BetrSichV und dem ÜAnlG und den zugehörigen technischen Regeln, insbesondere der TRBS 1115-1. Die Einführung der einzelnen Prüfschritte erfolgt zeitlich gestaffelt.

Die Überprüfung der Wirksamkeit von CS-Maßnahmen gemäß TRBS 1115-1 Abschnitt 5 und der Kontrollen gemäß TRBS 1115-1 Abschnitt 8.2 sind nicht Bestandteil der nachfolgend beschriebenen Prüfung durch die ZÜS.

Die zugelassene Überwachungsstelle kann sich die durch die Anwendung eines Managements der Cybersicherheit erzeugten Ergebnisse zu eigen machen. Wird kein Management der Cybersicherheit nach TRBS 1115-1 Anhang 1 angewendet, kann sich die zugelassene Überwachungsstelle die

Ergebnisse der Überprüfung der Wirksamkeit der CS-Maßnahmen zu eigen machen, wenn Durchführung und Ergebnis der Überprüfung für sie plausibel und nachvollziehbar sind.

Die Prüfung der Eignung von CS-Maßnahmen setzt einen strukturierten und dokumentierten Prozess des Arbeitgebers voraus. Die Dokumentation hierzu ist zur Prüfung vorzulegen. Ein Beispiel, wie dieser Prozess vom Arbeitgeber durchgeführt und zusammenfassend dokumentiert werden kann, ist als Anhang beigefügt.

4.1 Prüfung im Erlaubnisverfahren

Es ist zu prüfen, ob der Antragsteller Aspekte der Cybersicherheit in den für das Erlaubnisverfahren zu prüfenden Unterlagen entsprechend den Anforderungen der TRBS 1115-1 angemessen berücksichtigt hat.

4.2 Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung durch eine ZÜS

4.2.1 Allgemein

(1) Aus der TRBS 1115-1 ergeben sich die folgenden Prüfinhalte:

- Eignung und Funktionsfähigkeit der CS-Maßnahme,
- Plausibilität der Dokumentation und der Festlegung der erforderlichen CS-Maßnahmen,
- Feststellung, ob ein Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus vorhanden ist.

(2) Die Prüfung der Eignung der CS-Maßnahmen erfolgt in Form einer Plausibilitätsprüfung des Prozesses gemäß TRBS 1115-1 Abschnitt 4.4.3.

4.2.2 Prüfumfang

(1) Bis zum 31. März 2024 ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.

(2) Ab dem 1. April 2024 wird eine Plausibilitätsprüfung der Prozesse zur Planung und Realisierung der CS-Maßnahmen durchgeführt. Insbesondere sind hierbei die in den folgenden Absätzen dargestellten Punkte zu prüfen.

(a) Sind die sicherheitsrelevanten MSR-Einrichtungen und weitere schutzbedürftige Einrichtungen erfasst und dokumentiert?

Hinweis: Im Rahmen der Prüfung durch die ZÜS sind hinsichtlich der Cybersicherheit insbesondere die sicherheitsrelevanten MSR-Einrichtungen, die für den sicheren Betrieb erforderlich sind (vgl. z.B. TRBS 1201-x, TRBS 1115, EK ZÜS Beschluss BE-006) und auch im Rahmen der klassischen Anlagen-/Anlagenteilprüfung geprüft werden, einschließlich relevanter Teile der IT-/OT-Umgebung, zu betrachten.

(b) Wurden mögliche Auswirkungen auf die Integrität und Verfügbarkeit der Einrichtungen durch Cyberbedrohungen ermittelt und bewertet?

Hinweis: Die Bewertung der möglichen Auswirkungen erfolgt ohne Berücksichtigung von bereits bestehenden oder geplanten CS-Maßnahmen.

(c) Sind nachvollziehbare Festlegungen von CS-Maßnahmen für die Einrichtungen getroffen, um die geforderte Funktionsfähigkeit sicher zu stellen, und sind sie plausibel?

- Gibt es eine dokumentierte Festlegung der erforderlichen Maßnahmen der Cybersicherheit (Ja / Nein). Wenn ja, wurden die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 behandelt?
- Sind Herstellervorgaben vorhanden und wenn ja, wurden diese berücksichtigt?

(d) Gibt es Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus (z. B. Aufspielen von Software-Updates oder sicherheitsrelevanten Patches)?

(e) Wurden die Vorgaben für die organisatorischen CS-Maßnahmen in Betriebsanweisungen umgesetzt?

(f) Wurde die mögliche Beeinträchtigung der Wirksamkeit der sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen durch die festgelegten CS-Maßnahmen und deren Umsetzung betrachtet (Rückwirkungsfreiheit)?

(3) Die Prüfung der Funktionsfähigkeit der CS-Maßnahmen im geeigneten Umfang erfolgt zu einem späteren Zeitpunkt.

4.3 Wiederkehrende Prüfung

4.3.1 Allgemein

Die erstmalige Prüfung der CS-Maßnahmen bei einer Anlage, die wiederkehrend gemäß § 16 BetrSichV geprüft wird, erfolgt sinngemäß nach Abschnitt 4.2, inklusive der dort festgelegten Prüfumfänge.

4.3.2 Prüfumfang

(1) Bis zum 31. März 2024 ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.

(2) Ab dem 1. April 2024 ergeben sich die folgenden Prüfinhalte:

- Sind die vorgesehenen CS-Maßnahmen weiterhin geeignet?
- Liegen Vorgaben zur regelmäßigen Kontrolle der CS-Maßnahmen vor und werden diese durchgeführt?
- Sind Nachweise der Kontrolle der technischen und organisatorischen CS-Maßnahmen vorhanden?
- Werden anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, z. B. nach bekanntgewordenen Sicherheitslücken oder aus dem fortschreitenden Stand der Cybersicherheitstechnik berücksichtigt?
- Wurden falls erforderlich Anpassungen an den CS-Maßnahmen vorgenommen?
- Wurden prüfpflichtige Änderungen an der überwachungsbedürftigen Anlage hinsichtlich der Auswirkungen auf die erforderlichen CS-Maßnahmen bewertet?

(3) Die Prüfung der Funktionsfähigkeit der CS-Maßnahmen im geeigneten Umfang erfolgt zu einem späteren Zeitpunkt.

5 Mängeleinstufung

Nachfolgend sind ergänzend zu den bestehenden Vorgaben für die Mängeleinstufung Beispiele für eine Mängeleinstufung im Rahmen der Prüfung der Cybersicherheit dargestellt.

Geringfügiger Mangel:	Die Dokumentation zur Behandlung von Cyberbedrohungen wurde nicht vorgelegt, ist unvollständig oder fehlerhaft.
Erheblicher Mangel:	Es gibt ungeschützte Verbindungen von schutzbedürftigen Systemen in unzureichend geschützten Bereichen, die zu Gefährdungen führen können.
Gefährlicher Mangel:	Eine Kompromittierung von schutzbedürftigen Systemen, die zu Gefährdungen führen kann, ist bereits erfolgt.

Anhang

Beispielhafter Ablauf zur Planung und Realisierung erforderlicher Cybersicherheitsmaßnahmen

Hinweis: Handelt es sich beim Betrachtungsgegenstand um ein verwendungsfertiges System zur Umsetzung einer Sicherheitsfunktion mit durch den Hersteller bestätigter Cybersicherheit, ist gemäß TRBS 1115-1 eine Planung und Realisierung von Maßnahmen der Cybersicherheit durch den Betreiber nicht erforderlich. Maßgeblich für die Cybersicherheit im Betrieb ist in diesem Fall die Einhaltung der Vorgaben des Herstellers, die z. B. in Form einer Betriebsanleitung dargelegt sind.

Die folgenden Schritte beschreiben einen Ablauf zur Ermittlung der erforderlichen Cybersicherheitsmaßnahmen.

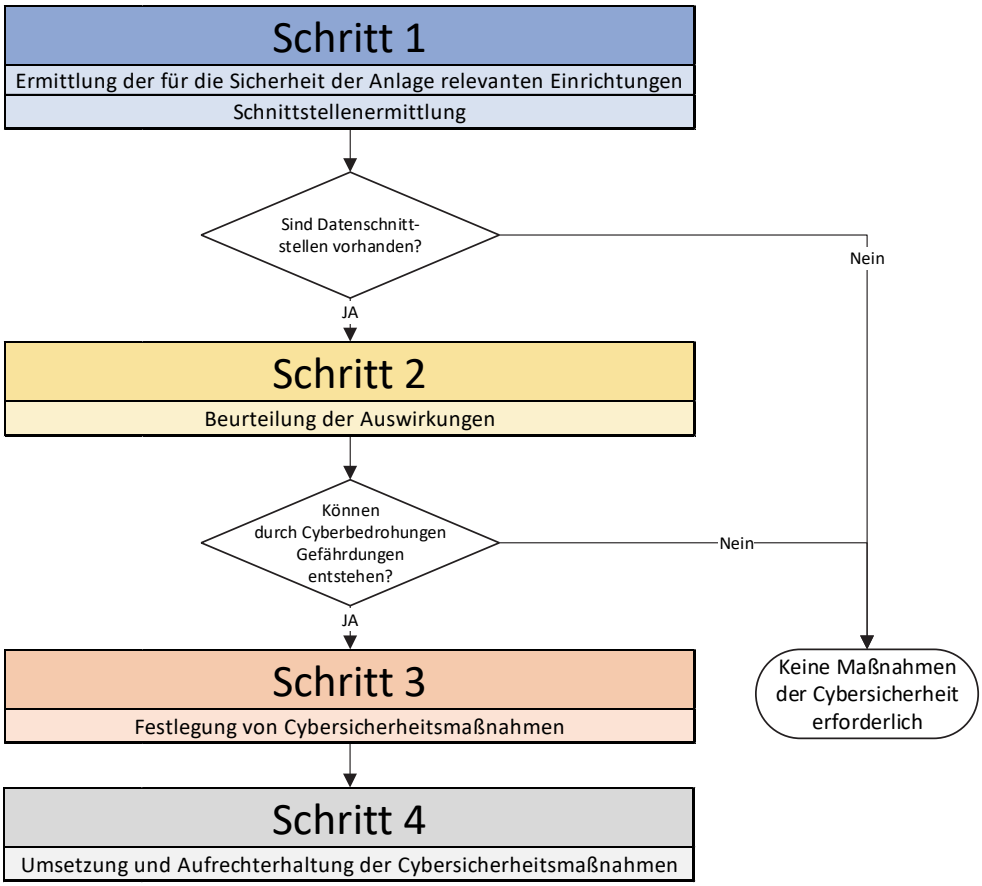

Abbildung 2: Ablauf zur Ermittlung der erforderlichen Cybersicherheitsmaßnahmen

Auf eine detaillierte Beurteilung der Auswirkungen von Cyberbedrohungen (Schritt 2) kann verzichtet werden, wenn pauschal ein anforderungsgerechter Schutzbedarf festgelegt wird.

Eine Konkretisierung der Inhalte der Schritte 1 bis 4 ist in den folgenden Tabellen enthalten.

Beispielhafte zusammenfassende Dokumentation des Prozesses zur Planung und Realisierung der Cybersicherheitsmaßnahmen:

Schritt 1	
Ermittlung der für die Sicherheit der Anlage relevanten Einrichtungen	**Schnittstellenermittlung**
Benennung der jeweiligen sicherheitsrelevanten MSR-Einrichtung / Schutzeinrichtung / des Ausrüstungsteils mit Sicherheitsfunktion, autarken Sicherheitseinrichtung oder des Anlagenteils, das hinsichtlich möglicher Auswirkungen von Cyberbedrohungen auf den sicheren Zustand der Anlage zu untersuchen ist	**Benennung der an der Einrichtung vorhandenen Daten-Schnittstellen**
Einrichtung A	
Einrichtung B	
…	

Schritt 2			
Beurteilung der Auswirkungen von Cyberbedrohungen			
Benennung der betrachteten Einrichtung	**Kurzbeschreibung der Schutzfunktion / des Schutzziels**	**Durch die Folgen einer Manipulation (z. B. Fehl-Auslösung, Blockierung der Auslösung oder Parameter- oder Funktionsänderungen) können grundsätzlich Gefährdungen entstehen. (Ja/Nein) Wenn „Ja“ bitte beschreiben.**	**Es gibt folgende nicht digitale Maßnahmen, um die Folgen der Manipulation auf ein ungefährliches Maß zu reduzieren. (Eintragung nur, wenn zutreffend erforderlich)**
Einrichtung A			
Einrichtung B			
…			

Schritt 3					
Festlegung von Cybersicherheitsmaßnahmen					
Benennung der schutzbedürftigen Einrichtungen	**Die Elemente gemäß TRBS 1115-1 Abschnitt 3.2 sind im erforderlichen Umfang erfasst. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 wurden im erforderlichen Umfang berücksichtigt. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Eine Festschreibung der erforderlichen Cybersicherheitsmaßnahmen ist erfolgt. (Ja/Nein) (Spezifikation der Cybersicherheit) (zzgl. Verweis auf Dokumentationsort)**	**Wenn Herstellervorgaben zur Cybersicherheit vorhanden sind, werden diese berücksichtigt. (Ja/Nein)**	**Ein Verfahren zur Aufrechterhaltung des Cybersicherheits-niveaus ist festgelegt. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**
Einrichtung x					
Einrichtung x					
…..					

Schritt 4		
Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen		
Benennung der schutzbedürftigen Einrichtungen	**Organisatorische Maßnahmen der Cybersicherheit sind in einer Betriebsanweisung festgeschrieben (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Technische Maßnahmen der Cybersicherheit sind nachweislich funktionsfähig/wirksam (Ja/Nein) (siehe hierzu TRBS 1115-1 Abschnitt 5 und 8.2)**
Einrichtung x		
Einrichtung x		
…		

Andere Darstellungsformen (z. B. mit Gruppierungen von mehreren sicherheitsrelevanten MSR-Einrichtungen, Typisierungen von gleichartigen sicherheitsrelevanten MSR-Einrichtungen) oder inhaltsspezifische Verweise auf bereits etablierte Prozesse oder Dokumentationen können je nach Komplexität der Anlage sinnvoll sein. Entscheidend für die Durchführbarkeit der Prüfung ist die Verfügbarkeit der oben genannten erforderlichen Informationen.

Inhaltsverzeichnis