Kundeninformation

Hinweise und Hintergrundwissen zum Thema Cybersicherheit

Während die Digitalisierung in allen Bereichen des Lebens voranschreitet, versuchen weltweit agierende Hackerkollektive und Cyber–Kriminelle, in Netzwerke von Unternehmen und Verwaltungen einzudringen, um Daten zu manipulieren, zu stehlen bzw. Lösegeldforderungen zu stellen. Im Rechtsbereich der Betriebssicherheitsverordnung spielt der Arbeits- und Gesundheitsschutz von Beschäftigten und dritten Personen in Unternehmen die entscheidende Rolle. Dabei muss der Umgang mit Arbeitsmitteln sicher sein und dem Stand der Technik entsprechen. Die zunehmende Datenvernetzung und der steigende Automatisierungsgrad von Arbeitsmitteln erfordert sicherheitsrelevante Mess- Steuer- und Regeleinrichtungen (MSR), um die Arbeitsprozesse sicher zu gestalten. Wenn es Cyber–Kriminellen gelingt, die sicherheitsrelevanten MSR-Einrichtungen zu kompromittieren, dann kann das Unternehmen zum einen abhängig von ihnen werden und zum anderen sind die Mitarbeiter in Gefahr.

Welche Pflichten hat der Betreiber?

Zum Schutz vor solchen Manipulationen hat der Gesetzgeber am 22. März 2023 im Rechtsbereich der BetrSichV die Technische Regel 1115 Teil 1 veröffentlicht. Sie fordert vom Arbeitgeber, dass mögliche Cyber–Bedrohungen an Arbeitsmitteln und insbesondere an überwachungsbedürftigen Anlagen wie Aufzug-, Druck- oder Ex-Anlagen, im Rahmen von Gefährdungsbeurteilungen identifiziert und entsprechende Vorkehrungen und Schutzmaßnahmen getroffen werden müssen.

Während die Betriebssicherheitsverordnung für den Betreiber die gesetzlichen Anforderungen festlegt, werden in den Technischen Regeln zur Betriebssicherheitsverordnung (TRBS) diese Anforderungen konkretisiert. Bei Einhaltung der Technischen Regeln kann der Arbeitgeber insoweit davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

Für die Einarbeitung in das Thema Cybersicherheit und die dazugehörigen Betreiberpflichten haben wir für Sie am Ende eine Auflistung kostenloser Dokumente zusammengestellt.

Betrifft diese Thematik nur Anlagen oder Anlagenteile mit einer Internetverbindung?

Nein, die Betrachtung und Festlegung von Maßnahmen kann nicht auf Anlagen mit Internetverbindung reduziert werden, da es neben der Internetverbindung auch noch weitere Möglichkeiten für einen ungewollten Systemzugriff gibt.

Einen wesentlichen Angriffspunkt stellen die vorhandenen Schnittstellen dar – Um Zugriff auf ein System zu bekommen, könnten beispielsweise die an der Steuerung vorhandene USB-Ports genutzt werden. Über schlecht geschützte USB–Ports ist ein Eingriff ins System vielleicht sogar leichter möglich wie über eine gut geschützte Internetverbindung – Vorausgesetzt, der Angreifer hat überhaupt Zugriff auf die USB–Ports.

Aktuelle Informationen zur Cybersicherheit finden Sie auch unter **dekra.de/cybersicherheit**

10/2023

Bei der ersten Orientierung und richtigen Einordnung kann folgender Baum als Hilfestellung genutzt werden:

Ist die Einrichtung für den sicheren Betrieb der Anlage relevant?

Handelt es sich um eine sicherheitsrelevante (MSR–) Einrichtung, die als technische Schutzmaßnahme für die sichere Verwendung der Anlage eingesetzt wird? Diese könnten sein:

> Ausrüstungsteile mit Sicherheitsfunktion (Druckgeräterichtlinie)
> Ausrüstungsteile mit Sicherheitsfunktion (Aufzugsrichtlinie)
> Sicherheits- Kontroll- und Regelvorrichtungen (ATEX)
> Einrichtungen nach TRGS 725
> Autarke Sicherheitseinrichtungen, die keine MSR–Einrichtungen sind (z. B. Notrufsystem, Notbefehlseinrichtung, Frequenzumrichter mit Bremsüberwachung)

Hinweis: Die aufgezählten Punkte dienen der Veranschaulichung und ersetzen keine anlagenspezifische Betrachtung. Die TRBS 1115-1 und der EK ZÜS Beschluss B-002 liefern hier weitere Informationen über die zu betrachtenden Anlagen und Anlagenteile.

Nein

Ende der Betrachtung zum Thema Cybersicherheit

Ja

Können die in der Einrichtung hinterlegten, sicherheitsrelevanten Parameter geändert und gespeichert werden?

Denn die Gefahr entsteht erst, wenn die vom Hersteller vorgegebenen oder dem Betreiber eingestellten Parameter verändert werden können. Übrigens: Für einen Cyberangriff benötigt ein Krimineller neben dem notwendigen Fachwissen zusätzlich auch eine Zugriffsmöglichkeit auf die sicherheitsrelevante Einrichtung.

Ein Angriff kann beispielsweise über folgende Zugriffsmöglichkeit erfolgen:

> Kabellose Schnittstelle (z. B. WLAN, Bluetooth)
> Kabelgebundene Schnittstelle (z. B. LAN, BUS, USB-Port, Bedienschnittstelle)
> Internetanbindung
> Remote-Zugriff/Zugang für Fernwartung
> Unbefugter Zugang zur Anlage/Schnittstellen

Nein

Ende der Betrachtung zum Thema Cybersicherheit

Weiter, wenn beide Bedingungen erfüllt sind

Eine Betrachtung der Cybersicherheit muss erfolgen, die Festlegung der Cybersicherheitsmaßnahmen ist der ZÜS mitzuteilen.

Zukünftig ist die Cybersicherheit Bestandteil der ZÜS Prüfung, doch was wird hier eigentlich geprüft?

Aufgrund der Komplexität des Themas haben sich die ZÜSen auf eine mehrstufige Einführung von Prüfvorgaben verständigt. So hat der Betreiber genügend Zeit, sich mit diesem in der Regel neuen Thema in Ruhe zu befassen und die notwendigen Unterlagen zu erarbeiten.

Die Sachverständigen der DEKRA prüfen daher ab dem 01.07.2023 ob sich der Betreiber in Bezug auf seine Anlage bereits mit dem Thema Cybersicherheit beschäftigt und dies dokumentiert hat. Dabei ist es zum jetzigen Zeitpunkt noch unerheblich, welches der bekannten Verfahren hierbei angewendet wurde. Dem Sachverständigen reicht der Nachweis, dass eine entsprechende Betrachtung durch den Betreiber dokumentiert durchgeführt wurde, eine inhaltliche Prüfung findet noch nicht statt. Sie können hierfür bis zum 01.04.2024 unser Formblatt auf **dekra.de/cybersicherheit** nutzen.

In der ab dem 01.04.2024 geplanten zweiten Stufe kann sich dieses Vorgehen ändern – der Sachverständige wird die Dokumente nun voraussichtlich auch inhaltlich auf Vollständigkeit und Plausibilität prüfen.

Übrigens: Die Entwicklung der Prüfvorgaben und zukünftigen Stufen findet aufgrund der Aktualität des Themas fortlaufend und dynamisch statt. Sie können sich über den aktuellen Stand im Beschluss B-002 des EK ZÜS unter folgendem Link informieren:
Beschlüsse des Erfahrungsaustauschs zugelassener Überwachungsstellen

Liste von hilfreichen Dokumenten bei der Einarbeitung in das Thema:

Wir weisen darauf hin, dass die DEKRA als zugelassene Überwachungsstelle keine Rechtsberatung und Unterstützung bei der Gefährdungsbeurteilung anbieten darf und die nachfolgende Auflistung daher nur als unvollständige und unverbindliche Empfehlung angesehen werden kann.

Betriebssicherheitsverordnung

> Die Betriebssicherheitsverordnung (BetrSichV) regelt in Deutschland die Bereitstellung von Arbeitsmitteln durch den Arbeitgeber, die Benutzung von Arbeitsmitteln durch die Beschäftigten bei der Arbeit sowie die Errichtung und den Betrieb von überwachungsbedürftigen Anlagen im Sinne des Arbeitsschutzes.

TRBS 1111 – Gefährdungsbeurteilungen

> Diese Technische Regel soll den Arbeitgeber im Hinblick auf die Vorgehensweise bei der Durchführung der Gefährdungsbeurteilung nach § 3 Betriebssicherheitsverordnung (BetrSichV) unterstützen. Ziel der Gefährdungsbeurteilung ist es, die auftretenden Gefährdungen der Beschäftigten bei der Verwendung von Arbeitsmitteln zu beurteilen und daraus notwendige und geeignete Schutzmaßnahmen abzuleiten.

TRBS 1201 – Prüfung und Kontrolle von Arbeitsmitteln und überwachungsbedürftigen Anlagen

> TRBS 1201-1 Prüfung von Anlagen in explosionsgefährdeten Bereichen
> TRBS 1201-2 Prüfung im Gefahrenfeld Druckanlagen
> TRBS 1201-3 Instandsetzung an Geräten, Schutzsystemen, Sicherheits-, Kontroll- und Regelvorrichtungen im Sinne der Richtlinie 2014/34/EU
> TRBS 1201-4 Prüfung von Aufzugsanlagen

TRBS 1115 Teil 1 – Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

> Diese Technische Regel konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR–Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden.

> Die in dieser TRBS dargestellte Vorgehensweise zur Festlegung, Umsetzung und Prüfung von Cybersicherheitsmaßnahmen ist auch geeignet, um über sicherheitsrelevante MSR–Einrichtungen hinausgehende Teile des Arbeitsmittels (z. B. notwendige Kommunikationsmittel) oder andere technische Infrastrukturen gegen Cyberbedrohungen zu schützen, wenn dieses als Ergebnis der Gefährdungsbeurteilung als erforderlich angesehen wird.

EK ZÜS Beschluss B-002 – Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

> Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Arbeitgebers 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.

> Für Arbeitgeber oder Betreiber überwachungsbedürftiger Anlagen kann dieser Beschluss (insbesondere Kapitel 5) als Hilfestellung für geeignete Vorgehensweisen zur Festlegung erforderlicher CS–Maßnahmen dienen.