Sicherheitsupdate für überwachungspflichtige Industrieanlagen

Merkblatt KAS-44 – Leitsatz zum Schutz vor cyberspezifischen Angriffen

Von Jürgen Bruder, Karlheinz Russ und Christian Weber

Cyberattacken gefährden mehr als die IT-Infrastruktur. Ganze Produktionsanlagen oder Lagerstätten stehen im Fokus der Hacker. Betreiber überwachungspflichtiger Anlagen sollten deshalb auch das digitale Risiko nicht aus den Augen verlieren. Dabei gilt es, spezielle Anforderungen an den Schutz von industriellen Produktionsanlagen zu beachten. Mit dem Merkblatt KAS-44 bietet die Kommission für Anlagensicherheit erste Leitsätze zum Schutz vor cyberphysischen Angriffen.

© iStock / thitivong / TÜV Hessen

Digitale Bedrohungen stellen Betreiber von überwachungspflichtigen Industrieanlagen vor eine große Herausforderung. In einer immer tiefer vernetzten Produktion mit drahtlos kommunizierenden Sensoren wird die Frage nach der Sicherheit neu gestellt. Dabei wird deutlich: Mit der voranschreitenden Industrie 4.0 endet der Schutz von Fertigungsprozessen nicht am Werkstor. Um Mensch und Umwelt auch weiterhin zuverlässig vor Unfällen mit gefährlichen Stoffen zu schützen, muss der Sicherheitsbegriff erweitert werden.

Die Kommission für Anlagensicherheit (KAS) hat das Bedrohungspotenzial erkannt, das von Hackern ausgeht. Bereits im Herbst 2017 wurden deshalb Leitsätze zum Schutz vor cyberphysischen Angriffen veröffentlicht. Das Merkblatt KAS-44 erweitert die grundsätzlichen Pflichten für Betriebsbereiche, die von der Störfall-Verordnung (Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes) betroffen sind. Zu den allgemeinen Betreiberpflichten zählt der umfassende Schutz dieser Bereiche. Dabei müssen Eingriffe unbe-

fugter Personen berücksichtigt werden, sowohl physisch als auch informationstechnisch.

Vernetzte Produktion – vernetzte Bedrohung

Die betroffenen Betriebsbereiche mit gefährlichen Stoffen werden im Zuge der Industrie 4.0 zunehmend intern und extern vernetzt, etwa zur Fernwartung. Da sie potenzielle Angriffspunkte darstellen, benötigen sie eine entsprechende Absicherung. Die Cybersicherheit wird deshalb zu einem wichtigen Bestandteil im Sicherheitskonzept der betroffenen Anlagen. Um den Schutz angemessen zu gestalten, bezieht sich das Merkblatt KAS-44 nur auf Systeme mit sicherheitstechnischer Relevanz. Die Integration der Cybersicherheit in ein Managementsystem kann analog zur ISO-27000-Normenreihe erfolgen. Mit den Leitsätzen verfolgt die KAS das Ziel, Anlagenbetreiber auf Cyberangriffe vorzubereiten. Das Merkblatt KAS-44 adressiert daher speziell Organisationen und Betriebsbereiche, die noch nicht über die notwendige Security-Kultur verfügen. Davon betroffen sind beispielsweise Unternehmen der chemischen Industrie, Lager, Zulieferer oder Betreiber von Biogasanlagen.

Leitsätze fördern Sicherheit

Um ein nachhaltiges Bewusstsein für Cyberbedrohungen zu etablieren, wird IT-Sicherheit im Merkblatt KAS-44 zur Chefsache. Die Leitung eines Unternehmens ist nicht nur für die Sicherheitsstrategie verantwortlich, sondern auch für die Kommunikation der Konzepte an alle Mitarbeiter, die sich mit der Anlagensicherheit befassen. Dafür werden alle Beteiligten regelmäßig geschult. Die konkrete technische Umsetzung der eingeführten Cybersicherheitsverfahren ist Aufgabe der IT-Abteilungen. Die KAS empfiehlt dafür die Einführung eines Asset-Registers, in dem alle Teile und Komponenten verzeichnet sind, deren Manipulation eine mittelbare oder unmittelbare Auswirkung auf die funktionale Sicherheit der Anlage hat. Ein visualisiertes Netzwerkregister veranschaulicht zusätzlich die internen Kommunikationsbeziehungen zwischen den Assets. Beim Bau und Betrieb von Anlagen soll Informationssicherheit zudem künftig eine integrale Rolle spielen. Die Anforderungen werden bereits während der Planung vom Betreiber festgelegt. Anschließend soll ein Cyber-Risk-Managementsystem den konstanten Schutz gewährleisten. Darin enthalten sind auch die rechtzeitige Erkennung von IT-Sicherheitsvorfällen und eine wirksame Bekämpfung der Hackerangriffe.

Safety versus Security

Bei der Umsetzung der erforderlichen Safety- und Security-Aktivitäten konkurrieren jedoch die unterschiedlichen Interessen der Ingenieure. Im Safety-Bereich werden Schutzeinrichtungen in Expertenteams geplant. Dabei steht das „handfeste“ Vorgehen im Vordergrund, etwa die vereinbarten Safety-Verfahren mit den Anlagenverantwortlichen abzustimmen und den Mitarbeitern verständlich zu kommunizieren. Die Weitergabe der Informationen ist notwendig – auch damit Wartungstechniker auf die Anlage zugreifen können, gegebenenfalls sogar von außerhalb.

IT-Verantwortliche wollen hingegen den Zugang zu den Systemen möglichst einschränken. Die damit verbundenen Security-Prozesse werden vertraulich behandelt und im Hintergrund implementiert. Geplante Safety- und Security-Aktivitäten können sich deshalb aufgrund der verschiedenen Schutzzielbetrachtung sogar widersprechen. Um eine Lösung für diesen unsachgemäßen Zustand zu finden, sollten Safety- und Security-Verfahren aufeinander abgestimmt sein und in einen gemeinsamen Change-Management-Prozess integriert werden.

Unternehmen stehen daher vor der Aufgabe, ihren Fokus zu erweitern. Es reicht nicht aus, Industrie 4.0 nur als optimierte Produktion oder effizientes Anlagenmanagement zu denken. Vielmehr ist eine neue Definition der IT-Sicherheit gefragt. Es kommt darauf an, die idealen Sicherheitsmaßnahmen zu bestimmen und im gesamten Unternehmen anzuwenden. Erst dann besteht die Chance, die Problematik der konkurrierenden Sicherheitsschnittstellen nachhaltig zu lösen. Der Fernzugriff von diversen Geräten ist ohne erweiterte Sicherheitsstandards beispielsweise undenkbar. Hierzu gehört auch die Integration von Security-Aspekten in die wiederkehrenden Safety-Prüfun-

gen gemäß Betriebssicherheitsverordnung, etwa bei gebäudetechnischen Anlagen wie Aufzügen.

Analyse und Bewertung

Bei der Umsetzung der KAS-44-Leitsätze in Unternehmen mit überwachungspflichtigen Industrieanlagen sollte zunächst der Status quo ermittelt werden. Anschließend folgt eine Priorisierung der relevanten Assets innerhalb der untersuchten Netzwerke. Dabei ist es entscheidend, ein Asset-Register einzuführen, um ein möglichst objektives Ergebnis zu erhalten. Nachdem die relevanten Assets identifiziert sind, wird das Risikomanagement analysiert und bewertet. Vor allem die Vollständigkeit und die Abschätzung aller denkbaren Risiken spielt dabei eine entscheidende Rolle. Denn in den nächsten Entwicklungsschritten wird die IT-Infrastruktur testweise attackiert, im Idealfall mit realistischen Angriffssimulationen. Daraus ergeben sich zahlreiche Optimierungen, die anschließend im Unternehmen realisiert werden. Um die Sicherheit der Industrieanlagen auch digital zu gewährleisten, sollte der Prozess permanent fortgeführt und weiterentwickelt werden.

Geeignete Tools erleichtern diese anspruchsvollen Aufgaben um ein Vielfaches. Speziell für den Einsatz in Produktionsnetzwerken entwickelte Managed Services können die zu prüfende IT-Infrastruktur kontinuierlich überwachen und testen. Dabei werden unzählige verschiedene Methoden und Angriffsmuster verwendet und untereinander kombiniert, um die tatsächliche Sicherheit der Systeme in Echtzeit zu errechnen. Eine Gap- oder auch Lückenanalyse zeigt anschließend die mögliche Diskrepanz zwischen dem Ist-Zustand und dem angestrebten Ziel: dem umfassenden Schutz der überwachungspflichtigen Anlagen.

Externe Unterstützung

Damit die KAS-44-Leitsätze möglichst umfassend realisiert werden, bietet sich die Unterstützung externer Experten an. Denn Außenstehende haben einen neutralen Blick auf die Aufgabe – und verfügen zudem über die notwendigen Ressourcen, die für die anspruchsvollen Herausforderungen benötigt werden. So können sie Schwachstellen schnell identifizieren und bei den folgenden Aufgaben wie der Erstellung von Asset-Registern, dem Risikomanagement oder den Angriffssimulationen zur Seite stehen, um die Sicherheit systematisch zu verbessern.

Der Umsetzungsprozess beginnt idealerweise mit einem Workshop, in dem der Anlagenbetreiber und die Cybersecurity-Experten gemeinsam die Ziele für die Risikobeurteilung definieren. Auch der Umfang der Zusammenarbeit wird festgelegt. Allen Beteiligten muss klar sein, welche Prozesse und welche Geräte oder Steuerungen von der Untersuchung betroffen sind. Die erstellte Übersicht der Assets ist die Grundlage für die Risikobetrachtung, denn sie enthält alle relevanten Komponenten und Schnittstellen. Anschließend werden die Netzzugänge und die Netzwerkgrenzen erfasst. Sind all diese Informationen vorhanden, folgt der Test, ob und wie gut die IT-Infrastruktur vor aktuellen Angriffen von außen geschützt ist.

Fazit

Während der gesamten Planung und Umsetzung eines Sicherheitskonzepts gegen cyberphysische Angriffe kommt es darauf an, dass die jeweiligen Verantwortlichen vertrauensvoll zusammenarbeiten und sich nicht gegenseitig als Konkurrenz betrachten. Die enormen Herausforderungen der Industrie 4.0 erfordern Lösungen, bei denen die Safety mit der Security in Einklang gebracht wird. Nur dann können überwachungspflichtige Industrieanlagen auch weiterhin umfassend sicher betrieben werden.

Dipl.-Ing. (FH) Jürgen Bruder
juergen.bruder@tuevhessen.de

Dipl.-Ing. Karlheinz Russ
karlheinz.russ@tuevhessen.de

Christian Weber
christian.weber@infraforce.de
TÜV Technische Überwachung Hessen GmbH