atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 11-12 2021

Cyber-Resilienz: Warum der Schutz vor Cyberattacken nicht ausreicht

Felix Kahrau

Um Cyber-Resilienz im Umfeld vernetzter Automatisierungssysteme zu erreichen, ist mehr notwendig als die Umsetzung grundlegender Schutzmaßnahmen. Zusätzlich ist es erforderlich, die Möglichkeit eines erfolgreichen Cyberangriffs zu akzeptieren und sich darauf vorzubereiten. Die Betrachtung sollte zudem nicht an den Grenzen des Automatisierungssystems enden, sondern die betrieblichen Funktionen, die durch das System unterstützt werden, miteinbeziehen.

Kann ein technisches System bei Störungen oder Teilausfällen essenzielle Systemfunktionen weiterhin zuverlässig ausführen, gilt es klassischerweise als resilient. Zur Absicherung gegen technische Störungen und Umwelteinflüsse gibt es etablierte Maßnahmen, wie redundante Auslegung, automatische Fehlerkorrektur oder sichere Abschaltung (fail-safe). Diese Maßnahmen sind allerdings typischerweise nicht als Schutz gegen Cyberangriffe konzipiert. Anders als eine technische Störung oder ein Umwelteinfluss, wird ein Angreifer versuchen, die Schutzmaßnahmen gezielt zu umgehen, also z. B. alle redundanten Komponenten anzugreifen. Mitunter lassen sich Schutzmaßnahmen sogar für einen Angriff ausnutzen, z. B. indem Fehlerkorrekturmechanismen genutzt werden um das aus der Korrektur resultierende Endergebnis im Sinne des Angreifers zu beeinflussen.

Zur Absicherung vernetzter Automatisierungssysteme werden daher typischerweise ergänzende Cyber-Sicherheitsmaßnahmen umgesetzt. Die Anbindung an andere Netze, wie das Büronetz des Unternehmens oder das Internet, wird mithilfe von Firewalls abgesichert und Antivirus-Lösungen auf den IT-Systemen des Automatisierungssystems installiert. Diese präventiven Maßnahmen allein bieten aber ebenfalls nur gegen einfache Massenangriffe, z. B. durch breit gestreute Schadsoftware, ausreichenden Schutz. Das liegt daran, dass es für einen Angreifer ausreichend ist, eine oder wenige Sicherheitslücken zu finden, wohingegen die Verteidiger alle Angriffsmöglichkeiten identifizieren und beseitigen müssen. Erschwerend kommt hinzu, dass kontinuierlich neue Software-Schwachstellen und Angriffsmöglichkeiten entdeckt werden, gegen die es sich zu schützen gilt.

Vorbereitung auf Cybernotfälle

Um ein vernetztes Automatisierungssystem auch gegen Cyberangriffe resilient zu machen, ist daher mehr erforderlich als grundlegende Schutzmaßnahmen. Cyber-Resilienz bezeichnet die Widerstandsfähigkeit eines Automatisierungssystems gegen Cyberangriffe. Man kann auch sagen, resilienzsteigernde Maßnahmen führen zu einer Reduktion des Risikos, das aufgrund von Cyber-Bedrohungen entsteht.

Neben Schutzmaßnahmen, die im Wesentlichen die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs beeinflussen, sollten auch die Möglichkeiten zur Minderung der Auswirkungen eines solchen Angriffs betrachtet werden. Im ersten Schritt bedeutet dies zu akzeptieren, dass ein erfolgreicher Cyberangriff möglich ist und sich auf diesen Fall vorzubereiten.

Diese Notfallvorbereitung umfasst die Definition der maximal tolerierbaren Wiederanlaufdauer (*Recovery time objective*) und die Identifikation der für den Notbetrieb erforderlichen Rahmenbedingungen. Wichtig hierbei ist, den Fokus auf den Wiederanlauf der essenziellen, durch das Automatisierungssystem unterstützten Funktionen zu richten und nicht auf die Wiederherstellung des gesamten Automatisierungssystems. Essenzielle Funktionen in diesem Sinn sind die Prozess- oder Arbeitsschritte, die zur Erreichung des gewünschten Endergebnisses mindestens erforderlich sind. Auf dieser Basis kann identifiziert werden, welche Anlagenteile oder Maschinen für den Notbetrieb erforderlich sind und inwiefern diese isoliert wiederhergestellt und betrieben werden können (vgl. Abbildung 1).

Zudem sollten, wo immer dies möglich ist, vom Automatisierungssystem unabhängige Alternativen zur Aufrechterhaltung der essenziellen Funktionen im Notbetrieb identifiziert werden, z. B. Möglichkeiten zur manuellen Betriebsführung, Beschaffung von Zwischenprodukten oder Zwischenlagerung von Produkten. Sofern Teile des Automatisierungssystem für den Notbetreib essenziell sind, sollte auch die Verfügbarkeit und Integrität von Daten- und Systembackups für diese Teilsysteme sichergestellt werden.

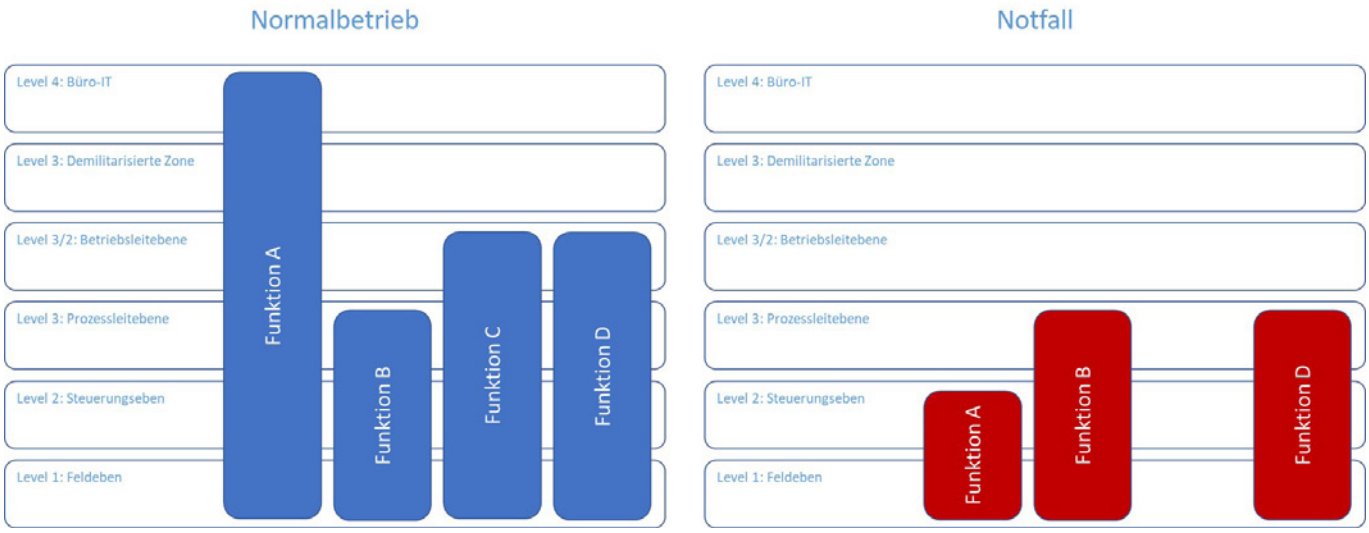

Abbildung 1: Automatisierungssystem und unterschützte Funktionen im Normalbetrieb und Notfall.

Die Wiederanlauffähigkeit sollte zudem regelmäßig getestet werden, um sicherzustellen, dass alle nötigen Vorbereitungen getroffen wurden, um den Wiederanlauf innerhalb der tolerierbaren Zeit tatsächlich gewährleisten zu können. Dies kann z. B. in Testumgebungen oder im Rahmen geplanter Stillstände erfolgen. Einzelne Schritte des Wiederanlaufs können mitunter separat getestet werden, etwa die Datenwiederherstellung aus Backups. Auch die Diskussion der Wiederanlaufpläne mit den beteiligten Fach- und Führungskräften anhand von Szenarien in Workshops (sog. *Table Top Excercises*) ist eine Möglichkeit.

Angriffserkennung und Reaktionsfähigkeit

Neben der Fähigkeit zur Wiederherstellung des Betriebs können die Auswirkungen eines Cyberangriffs auch reduziert werden, indem die Reaktionsfähigkeit verbessert wird. Dies umfasst den Aufbau von Maßnahmen zur Erkennung von Angriffen und die Erstellung von Incident-Response-Plänen, die die Verantwortlichkeiten und das Vorgehen im Ernstfall regeln.

Eine grundlegende Erkennungsfähigkeit kann typischerweise mithilfe vorhandener Daten etabliert werden. Durch regelmäßige Audits der Systemkonfigurationen und einen Prozess zur Auswertung bestehender Protokolle, z. B. von Firewalls und Antivirus-Lösungen, können bereits viele Cyberangriffe erkannt werden. Der Einsatz eines zentralen Protokoll-Servers und die Nutzung von Protokollanalyse-Tools können helfen diesen Prozess effizient zu gestalten. Eine umfassende Überwachung des Automatisierungsnetzes ermöglichen spezialisierte Systeme zur Anomalie- und Angriffserkennung. In der Praxis erfordert dies allerdings eine präzise an die Gegebenheiten der Anlage oder Maschine und die Erkennungsziele angepasste Konfiguration. Je mehr Anomalien und Angriffe erkannt werden sollen, desto höher ist auch die Rate der Falschmeldungen und damit der Aufwand zur Behandlung von Meldungen durch den Betreiber.

Reaktion auf Angriffe zeigt Nutzen auf

Der tatsächliche Nutzen der Angriffserkennung manifestiert sich aber erst durch Incident-Response-Fähigkeiten, d. h. durch die Fähigkeit auf Angriffsmeldungen angemessen zu

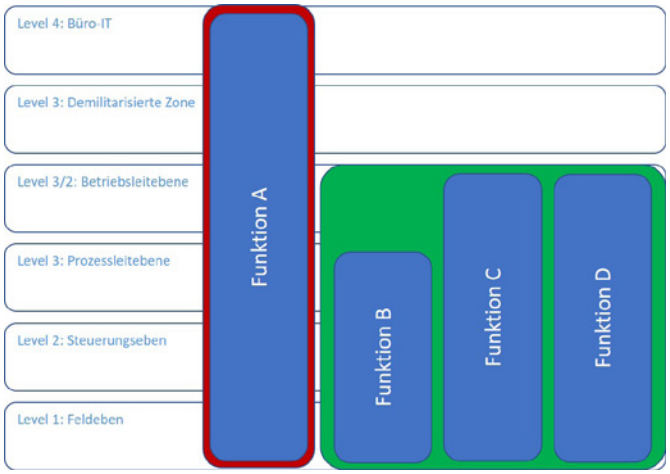

Abbildung 2: Die Isolierung der kompromittierten Funktion A.

reagieren. Incident-Response-Pläne sollten z. B. das Vorgehen im Falle einer Kompromittierung angrenzender Netzwerke, wie das Büronetzwerk des Unternehmens, regeln. Auch der Umgang mit einem Schadsoftwarebefall im Automatisierungsnetz sollte geplant werden. Relevante Fragen sind hierbei, wie lange ein Vorfall analysiert wird bevor weitere Schritte eingeleitet werden, wie die Ausbreitung eingedämmt sowie befallene Systeme identifiziert und bereinigt werden können.

Wie der Wiederanlauf sollte auch die Reaktionsfähigkeit eingeübt und regelmäßig getestet werden. *Table Top Exercises* bieten auch hier eine gute Möglichkeit Notfallszenarien mit allen Beteiligten abzustimmen und Incident-Response-Pläne zu diskutieren.

Resiliente Architektur des Automatisierungssystems

Die Auswirkungen eines Cyberangriffs können weiter reduziert werden, indem Überlegungen zu möglichen Cyberangriffen in die Architektur des Automatisierungssystems einfließen. Wesentliche Maßnahmen sind die Segmentierung des Netzwerks entsprechend der Funktion und Kritikalität der Komponenten sowie die Minimierung von Benutzerrechten. In einem umfassend segmentierten Automatisierungsnetz sind

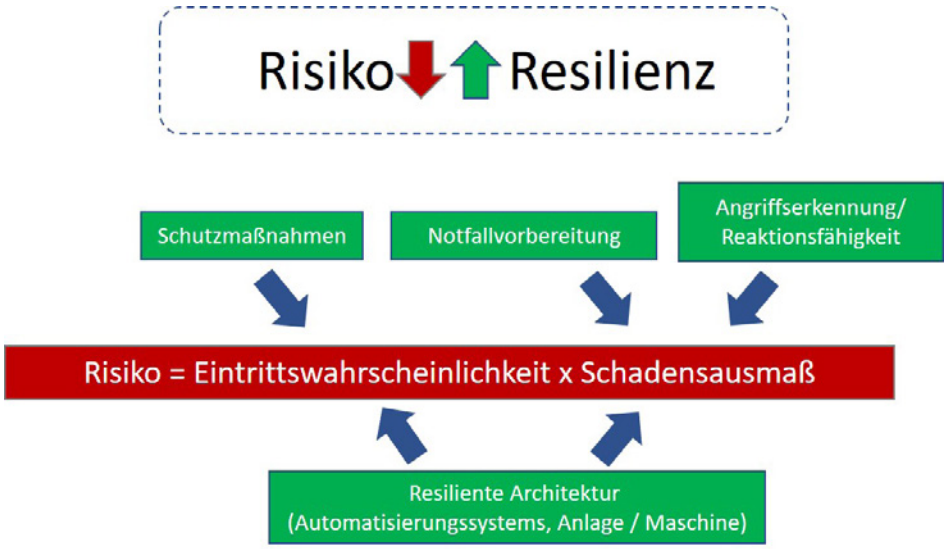

Abbildung 3: Der Zusammenhang zwischen Resilienz und Risiko.

die Komponenten entsprechend ihrer Funktion und Kritikalität separiert. Wie zuvor bezieht sich die Funktion nicht auf die Rolle der Komponente im Automatisierungssystem, sondern auf den unterstützten Prozess- oder Arbeitsschritt. Die Kritikalität einer Komponente ergibt sich aus ihrer Relevanz für die jeweilige Funktion, aber auch aus dem erwarteten Aufwand zur Wiederherstellung (Wiederanlaufzeit, Beschaffungskosten, etc.). Zudem sollte sich die Segmentierung an der Frage orientieren, wie gut die Segmentgrenzen und Übergänge zwischen den Segmenten geschützt und überwacht werden können.

Die Vergabe der Benutzerrechte sollte sich an der Benutzerrolle (Bediener, Techniker, Administrator, etc.) orientieren und nur die Berechtigungen umfassen, die für die Aufgabenerfüllung minimal erforderlich sind. Der Fokus auf die Benutzerrolle, nicht den Benutzer, ist hierbei elementar, d. h. ein Benutzter sollte für unterschiedliche Rollen auch verschiedene Benutzerkonten und Berechtigungen nutzen. Dies ist wichtig, um die Bewegungsfreiheit eines Angreifers nicht nur netzwerkseitig (durch Segmentierung), sondern auch bezogen auf die ausführbaren Handlungen bestmöglich einzuschränken. Ziel ist dabei nicht nur die unmittelbaren Auswirkungen eines Angriffs zu minimieren, sondern auch Angriffe zu verlangsamen und den Verteidigern so die erforderliche Zeit für eine effektive Reaktion zu verschaffen.

Cyber-Resiliente Maschinen und Anlagen

Auch bei der Konstruktion von Maschinen und Anlagen sind es nicht nur Cyber-Sicherheitsmaßnahmen, die helfen die Auswirkungen eines Angriffs zu minimieren. Konstruktionsbasierte Resilienz-Maßnahmen sind z. B. mechanische Schutzmaßnahmen, Verringerung der Abhängigkeit von der Automatisierungstechnik und prozessseitige Segmentierung.

Mechanische – nicht „hackbare“ – Schutzmaßnahmen sind eine naheliegende Möglichkeit die Auswirkungen eines Cyberangriffs zu reduzieren. Allerdings muss darauf geachtet werden, dass bewusste Manipulation und Angriffe bei der Auslegung der Maßnahmen explizit berücksichtigt werden.

Die Abhängigkeit von der Automatisierungstechnik in Notfallsituationen lässt sich z. B. reduzieren, indem Möglichkeiten geschaffen werden die Anlage bzw. Maschine manuell zu betreiben. Mitunter sind diese Möglichkeiten technisch bereits vorhanden, müssen aber noch durch Arbeitsabläufe ergänzt werden.

Die Segmentierung der Anlage bzw. Maschine auf Prozessebene, also eine Entkopplung von Prozess- oder Arbeitsschritten, kann auf unterschiedliche Weise zur Steigerung der Resilienz beitragen. Zum einen ermöglicht die Segmentierung die Aufrechterhaltung essenzieller Funktionen im Notbetrieb. Zum anderen werden die Handlungsspielräume im Incident-Response-Fall erweitert, da betroffene Segmente isoliert und damit das Gesamtsystem vor dem Angriff geschützt werden kann (vgl. Abbildung 2).

Fazit

Das Risiko, das aus Cyber-Bedrohungen resultiert, kann nicht nur durch präventive Maßnahmen auf ein akzeptables Niveau reduziert werden. Tatsächlich sind es auch nicht nur Cyber-Sicherheitsmaßnahmen, die zur Risikominimierung beitragen. Um Cyber-Resilienz zu erreichen ist es wichtig, die Möglichkeit eines erfolgreichen Cyberangriffs zu akzeptieren und sich darauf vorzubereiten. Dies kann durch Notfallplanung, Schaffen von Reaktionsfähigkeiten sowie architekturelle Verbesserungen auf Automatisierungssystem -und Prozessebene erfolgen (vgl. Abbildung 3). Die Fokussierung auf die essenziellen Funktionen, die durch das Automatisierungssystem unterstützt werden, erleichtert dabei die Umsetzung der Maßnahmen.

Dr. Felix Kahrau
anapur AG
67227 Frankenthal (Pfalz)
+49 6233 880393-15
f.kahrau@anapur.de