Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

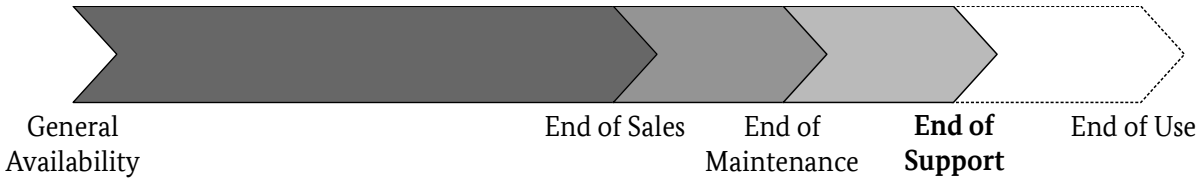
BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IN DER PRODUKTION

Umgang mit "End of Support" in industriellen Steuerungs- und Automatisierungssystemen

Industrielle Steuerungs- und Automatisierungssysteme (Industrial Control Systems, ICS) haben häufig eine sehr lange Lebenszeit. Nutzungsdauern von zehn oder mehr Jahren sind keine Seltenheit. Der Trend zum Einsatz von Systemen aus dem klassischen IT-Umfeld sorgt im industriellen Umfeld jedoch zunehmend für Probleme, denn diese sind meist auf kürzere Lebenszyklen ausgerichtet.

Systeme (Hardware, Firmware und Software) werden von den Herstellern nach Verkaufsende (End of Sales) oft noch einen weiteren Zeitraum mit Bugfixes und Sicherheitsupdates versorgt. Nach diesem Zeitraum (End of Maintenance) werden von manchen Herstellern noch schwerwiegende Sicherheitslücken geschlossen. Allerdings gibt es auch Produkte, zu denen bereits nach Verkaufsende keine Updates mehr angeboten werden. In diesem Dokument werden alle Systeme als „End of Support“ (EoS) bezeichnet, bei denen keine sicherheitskritischen Fehler und Schwachstellen mehr behoben werden.



End of Support im Produktlebenszyklus

EoS-Systeme sollten umgehend gegen noch unterstützte Versionen ausgetauscht werden, für die aktuelle Sicherheitsupdates bereitgestellt werden. Ein Weiterbetrieb darüber hinaus (End of Use) ist kein gewünschter Teil des Produktlebenszyklus. Einem Austausch können jedoch technische, betriebliche oder betriebswirtschaftliche Gründe entgegenstehen. EoS-Systeme sind - wie auch ungepatchte Systeme, die noch nicht EoS sind - grundsätzlich gefährdet, durch Angreifer oder Schadsoftware kompromittiert oder im Betrieb gestört zu werden.

Dieses Dokument soll einen Überblick über die Herausforderungen und Möglichkeiten eines möglichst sicheren Betriebes von EoS-Systemen geben. Es richtet sich an Systemintegratoren, Anlagenbauer und -betreiber im industriellen Umfeld.

1 Bewertung

Das BSI schätzt die Nutzung von EoS-Systemen als sehr kritisch ein. Für ältere Schwachstellen ist häufig Exploitcode oder Schadsoftware öffentlich verfügbar. Dies erleichtert auch weniger versierten Angreifern EoS-Systeme zu kompromittieren. Wenn sich der Weiterbetrieb solcher Systeme nicht vermeiden lässt, müssen zusätzliche Schutzmaßnahmen ergriffen werden. Ein Tausch gegen neuere Systeme muss geplant und vorgenommen werden.

Systeme mit direkter Erreichbarkeit aus dem Internet müssen besonders beachtet werden. Die-se können oft leicht über Suchmaschinen gefunden werden. Ein sicherer Weiterbetrieb solcher Systeme ist nach dem EoS so gut wie ausgeschlossen.

2 Abwägungen für den Austausch

Ein Austausch eines EoS-Systems durch eine neuere Version oder einen anderen Hersteller stellt in komplexen Anlagen eine Herausforderung dar. Dies reicht von unterschiedlichen Funktionalitäten bzw. Leistungsparametern bis zu fehlender Abwärtskompatibilität.

Bei fehlenden Funktionalitäten kann beispielsweise die eigentliche Funktion nicht mehr aufrecht erhalten werden. Es kann sich beispielsweise um eine spezielle Schnittstelle handeln, die in einem Folgeprodukt nicht mehr zur Verfügung steht. Es stellt sich dann die Frage, ob auch weitere Systeme getauscht werden müssen. Dies kann wiederum dazu führen, dass auch Anpassungen an der Software notwendig werden. Die Anpassung wiederum könnte eine Rezertifizierung der Anlage erfordern. Dies kann insgesamt mit so hohen Kosten verbunden sein, dass ein Tausch aus betriebswirtschaftlicher Sicht nicht sinnvoll erscheint.

Das Beispiel zeigt, dass der Austausch eines einzelnen Systems eine Reihe von weiteren Maßnahmen nach sich ziehen kann. Daher ist abzuwägen, ob das System wirklich ausgetauscht werden kann und ob alternative Maßnahmen getroffen werden müssen. Diese können ggf. eine weitere Nutzung des Systems ermöglichen. Es gilt jedoch, Gefährdungen zu reduzieren.

3 Maßnahmen

Die folgende Auflistung der Maßnahmen gibt einen Überblick zu verschiedenen Optionen und bewertet deren Vor- und Nachteile. Es muss beachtet werden, dass eine einzelne Maßnahme für einen ausreichenden Schutz meist nicht ausreichend ist und eine sinnvolle Kombination der Maßnahmen umgesetzt werden sollte. Diese Liste erhebt keinen Anspruch auf Vollständigkeit und soll erste Ansätze liefern.

Hinweis: Bei vielen der aufgelisteten Maßnahmen handelt es sich um Basismaßnahmen für ICS, die unabhängig von EoS-Systemen angewandt werden können und sollen.

3.1 Zugangsschutz

Der physische Zugang zu dem System und insbesondere den Schnittstellen sollte eingeschränkt werden. Auf diese Weise wird eine Kompromittierung durch externe Datenträger (z.B. USB-Sticks) erschwert. Jedoch kann über Netzwerkschnittstellen weiterhin Schadsoftware auf das System gelangen. Es handelt sich um eine Basismaßnahme, die grundsätzlich berücksichtigt werden muss.

Pro:

- Vergleichsweise einfach zu realisieren.
- Zuverlässiger Schutz vor physischen Angriffen.

Contra:

- Netzwerkverbindungen sind zusätzlich zu betrachten.

3.2 Netzwerkseparierung

Eine weitere Maßnahme stellt die Separierung des Systems durch Trennung sämtlicher Konnektivität (Air-Gap) zu anderen Systemen dar.

Pro:

- Technisch meist vergleichsweise einfach zu realisieren.
- Zuverlässiger Schutz vor Netzwerkangriffen.

Contra:

- Die Funktionsfähigkeit des Geräts kann stark eingeschränkt sein, beispielsweise ist eine Kommunikation und Übertragung von Daten (z.B. Prozessdaten oder Alarme) aus dem System nicht mehr möglich.
- Konfigurationen oder Parametrierung sind nur noch direkt am System möglich. Dies ist meist mit einem erhöhten Aufwand verbunden.

Hinweis: Dabei gilt zu beachten, dass auch temporäre Netzübergänge oder der Anschluss nicht vertrauenswürdiger Systeme wie Wartungslaptops, Datenträgern oder Programmiergeräten (z.B. zu Konfigurations- oder Wartungszwecken) ausreichen können, um das gefährdete System zu kompromittieren.

3.3 Datendioden

Der Einsatz von sog. Datendioden ermöglicht durch unidirektionalen Datenverkehr die Ausleitung von Prozessdaten und verhindert gleichzeitig Verbindungen hinein in das zu schützende Netzwerksegment.

Pro:

- Prozessdaten oder Alarme können vom System übermittelt werden, ohne dass die Gefahr eines unberechtigten Zugriffs über das Netzwerk besteht.
- Ein Rückkanal aus dem unsicheren Netz in das zu schützende System ist nicht möglich. Das Eintragen von Schadsoftware über diesen Weg ist somit ausgeschlossen.

Contra:

- Eine Konfiguration oder Parametrierung über das Netzwerk ist ebenso wie bei der Separierung nicht möglich.
- Aufgrund des fehlenden Rückkanals ist keine Quittierung eines korrekten Empfangs möglich. Somit sind nicht alle Netzwerkprotokolle über Datendioden realisierbar und Datenverlust bei der Übertragung kann nicht ausgeschlossen werden.

3.4 Logische Trennung

Eine logische Trennung lässt sich durch die Platzierung des betroffenen Systems in einem separaten Netzsegment erreichen. Der Datenverkehr zu diesem Netzsegment lässt sich mittels Firewall filtern und einschränken (Entwicklung eines geeigneten Zonenkonzepts [1, 2]).

In Systemen näher an der Feldebene (z.B. SPS, Sensorik, Aktorik) ermöglichen Protokollwandler zwischen verschiedenen Automatisierungsprotokollen oder Buskoppler (z.B. zwischen Ethernet und seriellen Protokollen) - sofern sie Funktions- und Weiterleit- ungsmöglichkeiten einschränken - eine logische Trennung zwischen Zonen in der Anlage.

Pro:

- Durch feingranulare Regelungen für den Zugriff lässt sich eine Gefährdung zeitlich und logisch minimieren.
- Durch Protokollwandler wird Schadsoftware, die nicht auf Automatisierungsprotokolle zielt, eine ungehinderte Ausbreitung im Netzwerk erschwert.
- Prozessdaten und Alarme können aus dem System übermittelt werden.

Contra:

- Der direkte Zugriff mittels Konfigurationswerkzeugen ist beim Einsatz von Protokollwandlern meist nicht mehr möglich.
- Aufwand für Wartung, Überwachung und Konfiguration ist für den weiteren Betrieb zu berücksichtigen.
- Durch organisatorische Mängel kann es zu Fehlkonfigurationen oder einer ungewollten Exponierung der Systeme kommen.
- Prinzipiell ist über jede Verbindung der Eintrag von Schadsoftware möglich.
- IP-basierte Protokollwandler können selbst kompromittiert werden und wiederum auf eine durch den Betreiber ungewollte Art und Weise beide Netzsegmente verbinden.
- Auch Firewalls und Gateways müssen aktuell gehalten und können selbst EoS werden

Hinweis: Eine einfache Möglichkeit stellen analoge oder digitale IO-Module einer Speicherprogrammierbaren Steuerung dar. Diese können genutzt werden, um eine begrenzte Anzahl von Informationen aus einem System auszuleiten. Notwendig ist jedoch eine Anpassung des Steuerungsprogramms und die Installation eines entsprechenden Empfangsmoduls.

3.5 Application Level Gateway

Als Ergänzung zu einer Firewall kann ein Application Level Gateway (ALG) eingesetzt werden. Das ALG fungiert als zusätzliche Kontrollinstanz. Während klassische Firewalls nur hinsichtlich der Kommunikationsverbindungen als Kontrollinstanzen agieren, werden die Verbindungen durch ein ALG terminiert und neu aufgebaut, womit zusätzlich eine inhaltliche Kontrolle des Datenverkehrs stattfinden kann.

Pro:

- Es kann eine Kontrolle der Inhalte des Netzwerkverkehrs stattfinden. Unabdingbar ist, dass das ALG auch eine semantische Prüfung (Deep Packet Inspection) der Protokollinhalte durchführen kann.
- Diese Funktionalität wird teilweise auch schon durch sog. Next-Generation-Firewalls angeboten. Es ist damit nur noch ein Gerät zu installieren.

Contra:

- Häufig werden ICS-Protokolle nicht oder nur rudimentär unterstützt.
- Protokolle mit Ende-zu-Ende-Verschlüsselung können nicht überwacht werden.

3.6 Jumphost

Ein Jumphost (auch Sprung- oder Rendezvous-Server genannt) ist ein zusätzliches System, das für den Zugriff genutzt wird [1]. Es dient ähnlich dem ALG dazu, die Verbindungen zu kontrollieren und Direktzugriffe auf das zu schützende System zu verhindern. Der Jumphost wird dabei als vertrauenswürdiges und entsprechend gehärtetes System (z.B. in Form eines SSH-, RDP- oder VNC-Servers) in einer demilitarisierten Zone (DMZ) betrieben, um nur von dort aus auf das EoS-System zuzugreifen.

Diese Maßnahme muss in Verbindung mit einer Firewall erfolgen.

Pro:

- Die Gefahr des Eintrags von einfacher Schadsoftware über das System zur Konfiguration wird reduziert.

Contra:

- Zusätzlicher Aufwand für den Betrieb des Jumphosts.
- Der Zugriff auf den Jumphost muss auf gehärtete und vertrauenswürdige Clients beschränkt werden.

3.7 Härtung der Systeme

Grundsätzlich sollten Systeme einer Härtung unterzogen werden bzw. bereits durch den Hersteller unterzogen worden sein. Bei der Härtung steht insbesondere eine sichere Grundkonfiguration im Fokus. Zusätzlich ist die Funktionalität auf das für den Anwendungsfall notwendige Minimum zu reduzieren. Dies bedeutet, dass sowohl ungenutzte als auch besonders gefährdete Dienste und Schnittstellen [2] deaktiviert werden und nicht benötigte Software deinstalliert wird.

Eine weitere Maßnahme zur Minimierung der Auswirkungen durch Schadsoftware ist der Einsatz von Anwendungsausführungskontrolle (engl. Allowlisting, AL) [1]. Dabei ist es nur erlaubt, bestimmte Anwendungen auszuführen.

Pro:

- Reduzierung der Angriffsfläche auf die zugelassenen Anwendungen und das AL selbst.
- Die Härtung ist teilweise mit Bordmitteln möglich.

Contra:

- Es fehlen vielfach Unterstützung und Dokumentation der Systeme hinsichtlich Maßnahmen zur Härtung. Teilweise können Dienste nicht deaktiviert werden oder es ist für den Betreiber mit erheblichem Aufwand verbunden, die entsprechenden Parameter für das AL zu bestimmen.
- Bei Systemupdates ist die Vertrauenswürdigkeit der Quellen sicherzustellen und die Konfiguration des AL zu aktualisieren (z. B. Prüfsummen, Zertifikate). Bei neuen Funktionalitäten (z.B. Programmen, Bibliotheken oder Verzeichnissen) besteht zudem die Gefahr, dass diese durch AL blockiert werden.

- Es kann nicht ausgeschlossen werden, dass mittels AL freigegebene Anwendungen selbst Schwachstellen beinhalten.

3.8 Monitoring und Protokollierung

Ein kontinuierliches Monitoring des gefährdeten Systems oder des Netzwerksegments [1], in welchem dieses betrieben wird, stellt insbesondere bei EoS-Systemen eine wichtige Maßnahme dar.

Die Protokollierung von Zugriffen [3] und Systemaufrufen, sowie die Überwachung des Netzwerkverkehrs mittels Application Level Gateway (z.B. in Verbindung mit einem Intrusion Detection System (IDS) [4]) können bei entsprechender Auswertung bei der Detektion von Angriffen unterstützen oder als Intrusion Prevention Systems (IPS) manche Angriffe verhindern.

Pro:

- Eine Kompromittierung kann ggf. frühzeitig festgestellt und unterbunden werden.

Contra:

- Monitoring kann eine Manipulation oder Infektion mit Schadsoftware nicht verhindern, sondern lediglich die Wahrscheinlichkeit einer Erkennung erhöhen.
- Intrusion Prevention Systeme können bei fehlerhafter Auslösung (false positive) zu Betriebsunterbrechungen führen.

3.9 Einsatz virtueller Maschinen

Insbesondere bei Computern mit Standardbetriebssystemen (z.B. Windows, Linux) geht der Trend zur Virtualisierung. Das hat betriebliche Gründe, ein Sicherheitsgewinn stellt diese Maßnahme jedoch nur dar, wenn zusätzliche Maßnahmen - beispielsweise im Hostsystem - getroffen werden.

Pro:

- Reduzierung der Abhängigkeit von Hardwareanforderungen oder fehlendem Support auf moderner Hardware.
- Das Erstellen von Snapshots vor Veränderungen erlaubt eine schnelle Wiederherstellung (siehe nächsten Abschnitt).

Contra:

- Kein Schutz vor Ausnutzung von Schwachstellen. Diese Maßnahme dient lediglich der Verbesserung der Verfügbarkeit. Es sind weitere Maßnahmen erforderlich, die eine Ausnutzung von Schwachstellen über das Netzwerk verhindern.
- Virtualisierung ist nicht für alle Systeme geeignet/möglich.
- Zeitkritische Anwendungen können meist nicht zuverlässig virtualisiert werden.
- Abhängigkeiten von spezieller Hardware, die nicht virtualisiert werden kann, sind zu beachten (z.B. I/O-Karten).

3.10 Backup und Recovery

Die Verfügbarkeit des Systems kann trotz aller Schutzmaßnahmen durch Angriffe gefährdet sein. Ein Backup- und Recovery-Konzept ermöglicht für den Fall einer Kompromittierung die Wiederherstellung aus einer Systemsicherung.

Pro:

- Schnelle Wiederherstellung im Problemfall möglich. Dies ist nicht nur im Fall von EoS-Systemen relevant und vorteilhaft.

Contra:

- Es besteht die Gefahr, dass auch Backups kompromittiert sind und man so Schadsoftware wieder einspielt oder die Backups unbrauchbar sind.
- Auch die Soft- und Firmware von Geräten kann kompromittiert werden und bedarf einer Berücksichtigung im Backupkonzept.

3.11 Ersatz bereithalten

Für mögliche technische Ausfälle (z.B. auf Grund der langen Einsatzdauer) sollte man durch die Bereitstellung von Ersatzteilen und -Geräten gerüstet sein. Dies ist insbesondere von Bedeutung, wenn es sich um alte Systeme handelt, die ggf. nicht mehr käuflich erworben werden können.

Pro:

- Es wird zusätzliche physische Redundanz geschaffen.

Contra:

- Der Betreiber muss bei EoS-Systemen den Einbau und die Konfiguration vollständig unabhängig vom Hersteller durchführen können, was bei einigen Systemen nicht möglich sein wird.

Lagerhaltung von „alten“ Systemen ist aufwändig. Zudem muss sichergestellt werden, dass die Systeme im Bedarfsfall auch noch einsatzfähig sind und durch die Lagerung selbst kein Schaden entsteht (z. B. Alterung von Elektronik, Ablauf von digitalen Zertifikaten).

4 Fazit

In jedem Fall sollte bei der Planung und Beschaffung von neuen Systemen bereits der EoS von einzelnen Komponenten oder eines ganzen Systems berücksichtigt werden. Spätestens jedoch vor End of Maintenance sollten zusätzliche Maßnahmen bereits implementiert werden, da ab diesem Zeitpunkt keine Herstellerunterstützung bei der Umsetzung von Maßnahmen mehr gegeben ist.

Eine Kombination aus obenstehenden Maßnahmen kann einen möglichst hohen Schutz bieten. Es sind nicht alle der genannten Maßnahmen in jedem Fall umsetzbar. Eine geeignete Kombination der umsetzbaren Maßnahmen kann jedoch eine Möglichkeit bieten, die Einsatzdauer von EoS-Systemen zu verlängern. Dies ist im Einzelfall zu prüfen und im Hinblick auf das Restrisiko zu bewerten.

Als weiterführende Literatur für die grundlegende Absicherung von Steuerungen und Industrieanlagen empfiehlt sich das ICS Security Kompendium des BSI [5].

5 Literatur- und Quellennachweis

[1] Umsetzungshinweise zum Baustein: IND.1 Prozessleit- und Automatisierungstechnik.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_IND_1_Prozessleit_und_Automatisierungstechnik.pdf?__blob=publicationFile

[2] Umsetzungshinweise zum Baustein: IND.2.1 Allgemeine ICS-Komponente.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_IND_2_1_Allgemeine_ICS_Komponente.pdf?__blob=publicationFile

[3] Fernwartung im industriellen Umfeld.

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf?__blob=publicationFile

[4] Monitoring und Anomalieerkennung in Produktionsnetzwerken.

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.pdf?__blob=publicationFile

[5] ICS-Security-Kompendium.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Leserinnen und Lesern an **service-center@bsi.bund.de** gesendet werden.