Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

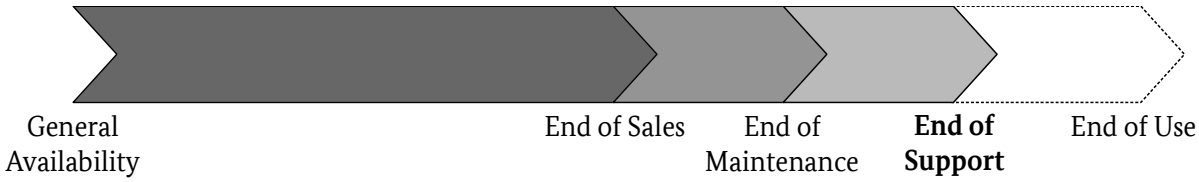
BSI-Veröffentlichungen zur Cyber-Sicherheit

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.

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□g Schadsoftware wieder□eingespielt oder die Backups unbrauchbar sind.
- • ¥È«Ë¯ æº•' • ä«)Ëíã¬ü• ëä *¯ú• ¯à Ú÷ää Úëã÷úëãÈ• Ë¯ú • ¯ú«¯à• ä« ¤¯«¬ú° ¯Ëã¯ú ¯ú ¥Ú þË¥È ËÃäÃËä ¬¥Ú÷þ<

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.