Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: INTEGRATOREN, MASCHINENBAUER

Sicherheitsspezifische Empfehlungen für Maschinenbauer und Integratoren

Durch die zunehmende Vernetzung von Maschinen und Anlagen in Anwendungsbereichen, wie der Fabrikautomation, sind diese inzwischen den gleichen Bedrohungen ausgesetzt, wie konventionelle IT-Systeme. Immer wieder kommt es zu Vorfällen bei denen Angreifer – meist über das Office-Netz des Unternehmens oder Fernwartungszugänge – bis ins Produktionsnetz vordringen. Um diesen neuen Bedrohungen ein angemessenes Sicherheitsniveau entgegensetzen zu können, bedarf es geeigneter Maßnahmen bei der Konzeption, Integration und dem Betrieb.

Herstellern oder Lieferanten der verbauten Komponenten kann die Verantwortung für den Umgang mit erkannten Schwachstellen nicht alleine angelastet werden. Auch der Betreiber einer Anlage kann die Verantwortung für einen hinreichend sicheren Betrieb nicht alleine übernehmen: Das entscheidende Bindeglied zwischen Herstellern und Betreibern sind die Maschinenbauer und Integratoren. Ihre Aufgabe ist es, durch geeignete Maßnahmen und Prozesse dafür zu sorgen, dass eine industrielle Anlage zu Beginn des Wirkbetriebs einem hinreichenden Sicherheitsniveau genügt. Dafür müssen sie dieses Sicherheitsniveau bis zur Inbetriebnahme gewährleisten und anschließend mit Wartungstätigkeiten und einem geeigneten Informationsfluss aufrechterhalten.

Die zentrale Rolle von Maschinenbauern und Integratoren wird in der Richtlinie 2182 „Informationssicherheit in der industriellen Automatisierung“ von VDI/VDE[1] aufgezeigt. Sie beschreibt modellhaft konkrete Schutzmaßnahmen anhand praxisnaher Beispiele. Durch einen prozessorientierten, zyklischen Ansatz werden dabei der gesamte Lebenszyklus und die Zusammenarbeit zwischen Herstellern, Integratoren und Betreibern berücksichtigt. Die folgende Abbildung veranschaulicht die in der Richtlinie 2182 enthaltenen Wechselwirkungen.

1 VDI/VDE 2182, http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/

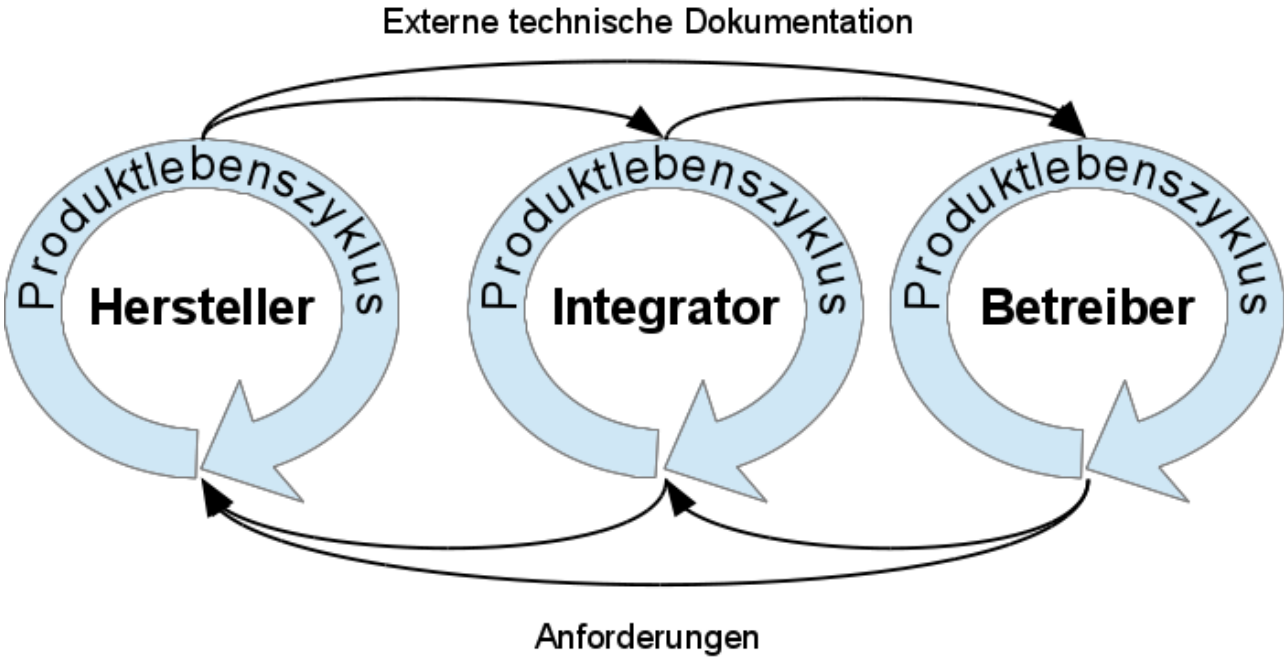

Abbildung 1: Lebenszyklen und Abhängigkeiten im Lebenszyklus einer Maschine / Anlage gemäß VDI/VDE 2182

1 Sichere Konzeption (Secure by Design)

Für einen sicheren Betrieb sollten Maschinenbauer und Integratoren die vom BSI definierten „Anforderungen an netzwerkfähige Industriekomponenten“[2] adaptieren und umsetzen. Die Veröffentlichung deckt von den Entwicklungsprozessen über technische Eigenschaften bis zur Dokumentation alle relevanten Aspekte ab.

- Allgemeine Vorgaben und Rahmenbedingungen für einen sicheren Betrieb
- Vorgaben zur sicheren Implementierung (Development Policies)
- Durchführung von Sicherheitsanalysen
- Sicherheit von Diensten und Schnittstellen
- Account-/User-Management, Sicherheit von Passwörtern und anderen Credentials
- Sichere Basiskonfiguration (Secure by Default)
- Backup & Restore
- Remote Access
- Schutz vor Schadsoftware
- Patchmanagement

2 Sichere Integration (Secure in Deployment)

Neben funktionalen Aspekten sollten auch Anforderungen an die Cyber-Sicherheit der Anlage von Beginn der Konzeption eingeplant und umgesetzt werden. Die folgenden Anforderungen können – meist unabhängig von den Kundenwünschen oder lokalen Gegebenheiten – immer realisiert und müssen nur geringfügig angepasst werden.

2 Anforderungen an netzwerkfähige Industriekomponenten, https://www.allianz-fuer-cybersicherheit.de/dok/6603528

- Horizontale und vertikale Segmentierung, beispielsweise durch Einsatz dedizierter Firewalls und Definition der Minimalanforderungen der Regelwerke für die in der Infrastruktur des Betreibers vorhandenen Firewalls und ggf. Unterstützung bei der Umsetzung
- Umsetzung flankierender Maßnahmen (z. B. Device Control, Schutz vor Schadsoftware, Logmechanismen, etc.)

Zudem sollten die Verantwortlichen kontinuierlich prüfen, ob durch den „Zusammenbau" unterschiedlicher Komponenten neue Bedrohungen entstehen, die von den Herstellern der Einzelkomponenten noch nicht entdeckt werden konnten.

3 Individuelle Anpassungen (Secure in Deployment)

Bei der Errichtung der Maschinen bzw. Anlagen beim Kunden sollten diese möglichst exakt an die für den jeweiligen Einzelfall geltenden Sicherheitsanforderungen und Bedingungen angepasst werden. Dazu sind besonders folgende Maßnahmen erforderlich, die gegebenenfalls von Integrator und Betreiber gemeinsam umzusetzen sind:

- Systemhärtung der Maschine bzw. Anlage und aller zugehörigen Komponenten (z. B. HMI oder Engineering Workstation) gemäß der Anforderungen und Gegebenheiten beim Kunden
- Aktivierung und ggf. Anpassung der vorhandenen Sicherheitsmechanismen mit anschließenden Funktions- und Sicherheitsprüfungen
- Erarbeitung von Policies für das Personal (z. B. Bediener) hinsichtlich Awareness, Umgang mit Wechseldatenträgern, etc.
- Erstellung einer Inventarliste der in der Maschine bzw. Anlage verwendeten Komponenten (Hard- und Software) und deren Versionen zur Aufnahme in das Sicherheitsmanagement beim Betreiber
- Aktualisierung des Netzplans beim Kunden
- Bereitstellung von Informationen, Anforderungen und identifizierten Restrisiken für einzelne Maschinen bzw. Anlagen zur Integration in ein Sicherheitskonzept bzw. Informationssicherheitsmanagementsystem (ISMS) des Betreibers. Ist ein solches Sicherheitskonzept nicht vorhanden, sollte der Integrator auf die Notwendigkeit eines solchen Konzepts hinweisen. Ggf. kann in diesem Fall auch eine erste Bewertung anhand der „ICS Top 10 Bedrohungen und Gegenmaßnahmen"[3] sowie dem darin enthaltenen Self Check erfolgen, um die verbleibenden Restrisiken aufzuzeigen.

Bei der Abnahme einer Maschine oder Anlage vor Ort (engl. Site Acceptance Test, SAT) kann zugleich eine Sicherheitsanalyse durchgeführt werden, um eine Aussage über den Status zum Zeitpunkt der Errichtung treffen zu können.

4 Maßnahmen zur Laufzeit

Nach erfolgter Integration einer Maschine oder Anlage ist die wichtigste Maßnahme das Nachhalten der Informationen zu Schwachstellen sowohl unmittelbar in der Implementierung als auch in Drittkomponenten (z. B. SPS oder Softwarebibliotheken).

3 ICS Top 10 Bedrohungen und Gegenmaßnahmen https://www.allianz-fuer-cybersicherheit.de/dok/6603554

Der Integrator sollte sich verpflichten, den Anlagenbetreiber über alle in dem Endprodukt verwendeten Komponenten zu informieren, da lediglich er diese Übersicht hat.

Im Fokus steht neben der zeitnahen Bereitstellung von Patches vor allem die Information der Kunden bzw. Betreiber. Oftmals ist die Installation von Patches nicht möglich oder mit erheblichem Aufwand verbunden. Daher ist es wichtiger, die Betreiber über Schwachstellen zu informieren. Diese können damit zur Optimierung des eigenen Risikomanagements beitragen und ggf. alternative Maßnahmen oder Workarounds aufzeigen. Weiterführende Informationen dazu liefert die Empfehlung „Handhabung von Schwachstellen“[4].

Darüber hinaus ist es erforderlich, Patches, Aktualisierungen und sonstige Softwarekomponenten sicher zur Verfügung zu stellen. Dies betrifft nicht nur die Absicherung der jeweiligen Downloads über Prüfsummen und Zertifikate, sondern auch die Sicherheit und Integrität der jeweiligen Webpräsenz.

Zudem sollten Patches zeitnah in die eigenen Produkte des Maschinenbauers bzw. Integrators integriert werden.

Schließlich sind die Betreiber möglichst frühzeitig und umfassend über geplante und anstehende Änderungen zu Support und Wartung (z. B. End-of-Service-Life, EOSL) zu informieren.

5 Weiterführende Informationen

Die folgenden weiterführenden Informationen liefern wertvolle Anregungen für eine intensive Beschäftigung mit den Anforderungen an Integratoren und Maschinenbauer sowie deren Umsetzungsmöglichkeiten:

- ICS Security Kompendium, https://www.bsi.bund.de/ICS-Security-Kompendium

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 Lesern an **info@cyber-allianz.de** gesendet werden.

4 Handhabung von Schwachstellen, https://www.allianz-fuer-cybersicherheit.de/dok/6603524