Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: HERSTELLER

Anforderungen an netzwerkfähige Industriekomponenten

Speicher-programmierbare Steuerungen (SPS) und ähnliche industriell genutzte, netzwerkfähige Komponenten verfügen zunehmend über Dienste, die auch bei Serversystemen zu finden sind. Sowohl diese allgemeinen Dienste als auch spezifische Funktionen der Automatisierungstechnik müssen angesichts der zunehmenden Vernetzung dieser Komponenten über ein hinreichendes Sicherheitsniveau verfügen. Dieses Dokument gibt Herstellern einen Überblick über die zentralen Best Practices für solche Komponenten. In Ergänzung hierzu stellt das BSI einen Leitfaden für Hersteller von Industriekomponenten zur Verfügung, der bei dem Aufbau von Produkttests und Sicherheitsanalysen unterstützen soll. Auch Maschinenbauer und Integratoren können dieses Dokument im Rahmen ihrer Produktentwicklung verwenden, um die sicherheitsspezifischen Anforderungen zu adressieren.

1 Organisatorische Maßnahmen

1.1 Product Lifecycle & interne Prozesse

Eine grundlegende Verbesserung der Sicherheit eines Produkts kann durch das Etablieren eines sicheren Entwicklungszyklus (Secure Software Development Lifecycle) erzielt werden. Hierzu kann man sich u. a. an den folgenden Fragen orientieren.

- Gibt es einheitliche und verbindliche, dem aktuellen Stand der Technik entsprechende Vorgaben zur sicheren Implementierung (Development Policies)?
- Sind im Entwicklungszyklus verbindliche Prüfphasen (Security Gates) vorgeschrieben, in denen beispielsweise ein Review der Anwendungslogik oder eine ganzheitliche Sicherheitsbetrachtung erfolgt?
- Sind – sofern technisch und wirtschaftlich möglich – automatisierte Codeanalysen fester Bestandteil des Entwicklungszyklus?
- Werden im Entwicklungszyklus Sicherheitsanalysen zu Bedrohungen und Risiken durchgeführt und Gegenmaßnahmen festgelegt?
- Werden Produkte abschließend bereinigt, sodass kein Test-Code aus dem Entwicklungsprozess mehr enthalten ist?
- Werden Produkte einer technischen Sicherheitsanalyse (Penetrations- oder Schwachstellentests) unterzogen, bei denen nicht nur auf bekannte Schwachstellen, sondern auch auf neue Verwundbarkeiten (z. B. durch Fuzzing-Tests) untersucht wird?

- Werden flankierende Sicherheitsmechanismen, beispielsweise zum Schutz vor Schadsoftware, gefördert (z. B. Zertifizierung) statt deren Einsatz z. B. durch einen Ausschluss der Gewährleistung zu untersagen?
- Gibt es einheitliche Regelungen zum Umgang mit Schwachstellen (vgl. BSI-Empfehlung „Handhabung von Schwachstellen“[1])?
- Haben Sie geeignete Prozesse etabliert, um Schwachstellen im verwendeten Betriebssystem, in Drittkomponenten sowie in Eigenentwicklungen nachzuhalten und so Rückschlüsse auf eine eventuelle Betroffenheit des eigenen Produkts zu schließen und geeignet zu reagieren?
- Werden Produkte über einen hinreichend langen Zeitraum möglichst zeitnah mit Patches und Updates versorgt, um entdeckte Schwachstellen zu beheben? Ist der Updateprozess für die Kunden möglichst effizient durchzuführen? Testen Sie Updates und Patches vor der Bereitstellung und garantieren Sie dafür, dass die Basisfunktionalität der Geräte dadurch erhalten bleibt? Informieren Sie Ihre Kunden darüber, welche Patches mit welcher Kritikalität zu bewerten sind?

Weitere sinnvolle Anforderungen, die im Rahmen eines sicheren Entwicklungsprozesses berücksichtigt werden sollten, finden sich u. a. im BDEW Whitepaper[2], bei WIB[3], in DIN SPEC 20009[4] oder in IEC 62443-2-4[5].

1.2 Kommunikation

In vielen Anwendungsbereichen, wie z. B. der Fabrikautomation oder der Prozesssteuerung, ist es wichtig, Integratoren und Betreiber möglichst umfassend und zeitnah mit geeigneten Informationen zu versorgen. Die Information über eine Schwachstelle kann häufig sehr viel wichtiger sein, als das Bereitstellen eines Patches. Daher sind die folgenden zentralen Fragestellungen zu betrachten.

- Bekennen Sie sich als Hersteller gerade mit Blick auf die Sicherheit ihrer Produkte zu einer möglichst offenen Kommunikation?
- Haben Sie Ansprechpartner oder Kontaktmöglichkeiten für Sicherheitsfragen / -vorfälle benannt, die möglichst 24/7/365 erreichbar sind? Haben Sie zudem Reaktionszeiten und Notfallprozeduren definiert (vgl. BSI-Empfehlung „Handhabung von Schwachstellen“[1])?
- Erfolgt eine möglichst effektive Benachrichtigung der Kunden, wenn eine Schwachstelle in einem Produkt bekannt wird?
- Führen Sie Informationen aus den unterschiedlichen Kommunikationskanälen, wie Hotline, Support, Foren, etc. zusammen, die evtl. auf Schwachstellen oder Vorfälle hinweisen könnten (z. B. Meldungen, wie „Auf meinem System wurde eine .dll-Datei ausgetauscht“)?

2 Produkteigenschaften

Die folgenden Mindestanforderungen an die Produkteigenschaften netzwerkfähiger Industriekomponenten sind als generische Empfehlung zu verstehen. In Abhängigkeit des konkreten Funktionsspektrums einer Komponente muss hier zunächst noch eine Anpassung erfolgen, beispielsweise wenn in einer Komponente kein Webserver bzw. keine Web-basierte Schnittstelle vorhanden ist.

1 https://www.allianz-fuer-cybersicherheit.de/dok/6603524
2 https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/
3 http://www.wib.nl/
4 https://www.beuth.de/de/technische-regel/din-iso-iec-tr-27019/223679647
5 http://webstore.iec.ch/

2.1 Dokumentation

Von besonderer Bedeutung für den sicheren Einsatz beim Kunden bzw. bei der Weiterverwendung durch Integratoren ist die Dokumentation des Produkts. Die folgenden Prüffragen sind als Orientierungshilfe bei der Erstellung und Überprüfung der Produktdokumentation geeignet. Weitere Anforderungen hierzu sind u. a. der VDI/VDE 2182[6] zu entnehmen.

1. Werden die Zielgruppen seitens eines Integrators oder Anwenders genannt, die aus sicherheitsspezifischen Überlegungen über die hier enthaltenen Informationen in Kenntnis gesetzt werden sollten?
2. Wird angemessen auf die Notwendigkeit hingewiesen, Standardpasswörter im Rahmen der Inbetriebnahme zu ändern?
3. Werden die Sicherheitseigenschaften bzw. -funktionen der Komponente beschrieben?
4. Stellen Sie dar, welche Risiken / Bedrohungen durch die Komponente selbst abgedeckt werden?
5. Sind sämtliche Schnittstellen, Zugänge und Funktionen dokumentiert?
6. Enthält die Dokumentation Informationen, auf deren Grundlage der Kunde ein Sicherheitskonzept erstellen kann?
   a) Ist dokumentiert, welche Bedrohungen im Rahmen einer Sicherheitsbewertung bzw. eines Sicherheitsmanagements zu beachten sind?
   b) Ist dokumentiert, wie diesen Bedrohungen entgegengewirkt werden kann?
   c) Ist dokumentiert, welche Dienste (mit den im Produkt integrierten Mechanismen) nicht abgesichert werden können und daher ergänzende technische oder organisatorische Sicherheitsmaßnahmen erfordern?
7. Gibt es Empfehlungen bzgl. der Konfiguration für einen sicheren Betrieb (z. B. Leitfaden zur Systemhärtung)?
   a) Gibt es ausreichende Hinweise für die Änderung von Standardpasswörtern und zum Deaktivieren von unbenötigten Accounts?
   b) Sind die sicherheitsspezifischen Konsequenzen der möglichen Konfigurationsoptionen / -alternativen dokumentiert?
   c) Gibt es Hinweise darauf, welche Einstellungen als kritisch zu betrachten sind und ggf. zu einer erhöhten Gefährdung führen?
   d) Gibt es eine Checkliste zur Übersicht über die Konfiguration und deren sicherheitsspezifische Implikationen?
8. Gibt es Referenzen auf weiterführende Informationen zur Absicherung bzw. zum sicheren Betrieb?Produktkonfiguration

Die Konfigurationsmöglichkeiten sind von besonderer Bedeutung für die Sicherheit einer Komponente, da hierüber u. a. Sicherheitsmechanismen gesteuert und parametriert werden. Hierzu sind insbesondere die folgenden Leitfragen zu beachten.

1. Erfolgt die Auslieferung in einer sicheren Basiskonfiguration?
2. Können unsichere / nicht-benötigte Dienste deaktiviert werden?
3. Sind die Passwörter, Zertifikate usw. für sämtliche Dienste austauschbar?
4. Kann die Konfiguration nur nach vorheriger Authentisierung modifiziert werden?

6 http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/

2.2 Technische Produkteigenschaften

Für einen sicheren Betrieb sind neben den Betreibern selbst auch die Hersteller verantwortlich. Praktikable sicherheitsspezifische Produktfunktionen sind ein wichtiger Baustein für eine ganzheitliche Absicherung.

1. Logging
   a) Wird verhindert, dass über Logdaten kritische Informationen (z. B. Logindaten) verbreitet werden?
   b) Werden alle ggf. kritischen Aktionen in Logdateien vermerkt wie z. B. die Änderung der Konfiguration, fehlgeschlagene Loginversuche, das Entfernen oder der Austausch von CF-Karten oder das Anschließen eines USB-Geräts?
2. Login / Authentisierung
   a) Gibt es eine feingranulare Zugriffskontrolle und eine hinreichende Benutzerverwaltung (d. h. mehrere Nutzer mit unterschiedlichen Rollen und Berechtigungen)?
   b) Werden Zugangsdaten (insbesondere Passwörter) statt als Klartext kryptografisch gemäß dem aktuellen Stand der Technik (z. B. keine Verwendung von MD5) geschützt gespeichert?
   c) Werden bei einem fehlgeschlagenen Login nur allgemeine Fehlermeldungen ausgegeben, die beispielsweise keinen Rückschluss darauf geben, dass der Username korrekt aber das Passwort falsch war?
   d) Erfolgt ein Timeout von Sessions bzw. kann dieser konfiguriert werden?
   e) Kann der Zugriff über die Netzwerkschnittstellen auf bestimmte MAC-Adressen oder IP-Adressen bzw. IP-Adressbereiche beschränkt werden?
   f) Gibt es ergänzende Mechanismen, die einen Eingriff durch einen Bediener absichern, wie z. B. Vier-Augen-Prinzip?
   g) Gibt es eine (temporäre) Sperre, einen SNMP-Alert o. ä., wenn ein Brute Force Angriff auf einen Loginmechanismus erfolgt?
3. Autorisierung
   a) Ist technisch ausgeschlossen, dass ggf. kritische Aktionen ohne das Vorhandensein der dazu erforderlichen Rechte ausgeführt werden können?
4. Weboberfläche
   a) Werden technische Maßnahmen ergriffen, um die Angreifbarkeit durch Cross Site Scripting (XSS) oder Cross Site Request Forgery (XSRF) zu erschweren bzw. zu verhindern?
   b) Ist es möglich, dass zumindest optional immer HTTPS für den Zugriff auf die Weboberfläche verwendet wird?
   c) Werden kritische Informationen immer verschlüsselt übertragen?
   d) Ist sichergestellt, dass Passwörter in der Konfiguration sowie beim Login niemals im Klartext angezeigt werden?
   e) Wird eine aktuelle Version des Protokolls SSL/TLS in einer aktuellen Implementierung verwendet? Insbesondere ist auf TLS 1.0 zu verzichten.

5. Netzwerkdienste

   a) Ist das Abschalten von Diensten (z. B. HTTP(S), FTP, etc.) und Schnittstellen (z. B. WLAN) möglich, wenn diese vom Integrator oder Betreiber nicht benötigt werden?

   b) Sind die Rechte minimiert, mit denen Dienste wie FTP oder der Webserver betrieben werden?

   c) Wurde die Implementierung insbesondere der grundlegenden Kommunikationsprotokolle hinsichtlich der Fehlertoleranz und Robustheit getestet (vgl. ISA 99)?

   d) Gibt es Vorkehrungen, um einen Angriff auf die Verfügbarkeit von Diensten durch Öffnen von vielen Verbindungen bzw. Sitzungen zu erschweren?

   e) Werden sämtliche Schnittstellen zum Gerät mit einer hinreichenden Eingabevalidierung abgesichert, um Manipulationen zu verhindern?

   f) Wird möglichst auf fehleranfällige Eigenimplementierungen von Diensten (z. B. Embedded Webserver) verzichtet?

6. Sonstiges

   a) Kann eine Fernwartung bzw. ein Schreibzugriff auf die Komponente nur dann erfolgen, wenn diese explizit aktiviert wird – beispielsweise über Schlüssel- oder Kippschalter?

   b) Werden – soweit verfügbar – sichere Alternativen zu verbreiteten Industrie-spezifischen Protokollen verwendet, wie z. B. Secure DNP3 statt DNP3 oder OPC UA statt OPC?

   c) Ist das verwendete Betriebssystem einer grundlegenden Systemhärtung unterzogen worden?

   d) Ist sichergestellt, dass bei einem Denial-of-Service Angriff die grundlegende Funktionalität der Komponente erhalten bleibt und die Komponente nach einem solchen Angriff den normalen Betrieb mit dem vollständigen Funktionsumfang wieder aufnimmt?

   e) Sind sichere und nutzerfreundliche Mechanismen für Backup und Wiederherstellung implementiert?

   f) Sind Update-Mechanismen (z. B. für Firmware-Updates), die über ein Netzwerk statt lokal am Gerät erfolgen, hinreichend abgesichert? Neben Integritätsprüfungen mittels Prüfsummen ist insbesondere eine geeignete Authentisierung oder eine Absicherung über Signaturen vorzusehen.

   g) Werden allgemein anerkannte Algorithmen und Implementierungen für kryptografische Verfahren genutzt, statt solche selbst zu entwickeln?

   h) XML-basierte Datenformate werden neben der Web-Kommunikation häufig für die Datenhaltung für eine Produktkonfiguration verwendet. Wird hierzu ein sicherer XML-Parser in einer restriktiven Konfiguration verwendet? Werden ergänzende Prüfungen von XML-Dateien durchgeführt, um XML-spezifische Angriffe[7] zu verhindern?

   i) Gibt es eine Möglichkeit zur automatischen Alarmierung im Falle von kritischen Systemereignissen oder -zuständen?

7 http://www.ws-attacks.org

Weitere Empfehlungen – insbesondere für eine HTTP(S)-Schnittstelle (Weboberfläche) – finden sich in der BSI-Empfehlung „Entwicklung sicherer Webanwendungen“[8], wobei dort insbesondere der Abschnitt "Entwicklungsphase" relevant ist.

2.3 Umsetzungsmöglichkeiten für ausgewählte Funktionen

Die konkrete Umsetzung von sicherheitsspezifischen Produkteigenschaften ist besonders sorgfältig zu konzipieren. Wichtig sind neben einer hinreichenden Qualität der Implementierung und dem damit erreichten Sicherheitsniveau auch Aspekte, wie beispielsweise die Auswirkungen mit Blick auf die Aufwände für Integratoren und Betreiber.

Hinweis: Die folgenden Ausführungen beleuchten einige konkrete sicherheitsspezifische Produktfunktionen und deren Umsetzungsmöglichkeiten. Hierbei handelt es sich um ausgewählte Beispiele, die in Zusammenarbeit mit Industriepartnern sukzessive erweitert werden. Anregungen und Ergänzungen nehmen die Autoren über ics-sec@bsi.bund.de entgegen.

Defaultpasswörter

Die Auslieferung eines Produktes mit Standardpasswörtern ist immer ein Sicherheitsrisiko. Hierzu gibt es eine Reihe von Lösungsmöglichkeiten, wie z. B.

- Hinweis in der Dokumentation – möglichst an herausragender Stelle – dass ein Standardpasswort gesetzt ist und dieses dringend geändert werden muss.
- Hinweis in der Administrationsoberfläche, dass ein Standardpasswort gesetzt ist.
- Erzwingen der Änderung bei Installation bzw. initialer Konfiguration.
- Auslieferung erfolgt bereits mit individuellem Passwort (z. B. abgeleitet von Seriennummer und MAC-Adresse), welches nach Factory Reset wieder gesetzt wird.

Zusätzlich zu den genannten Umsetzungsmöglichkeiten gibt es weitere flankierende Maßnahmen, wie z. B. das Empfehlen von Anforderungen an sichere Passwörter in der Dokumentation oder die technische Durchsetzung solcher Passwort Policies.

FTP und Alternativen

Das klassische FTP für den Dateitransfer verfügt über keine Sicherheitsmechanismen und ist daher unter Sicherheitsaspekten nicht zu empfehlen. Als mögliche Alternativen bieten sich z. B. das Secure File Transfer Protocol (SFTP) oder FTP über SSL bzw. TLS (FTPS) an. SFTP basiert auf SSH und bildet genau genommen eine Teilfunktionalität von SSH zum File-Transfer. Es hat – abgesehen von dem Zweck des Dateiaustauschs – mit dem eigentlichen FTP-Protokoll nichts gemeinsam. Entsprechend braucht SFTP – im Gegensatz zu FTP – nur eine Verbindung und läuft wie SSH über den Port 22, was gegenüber FTPS (s. u.) eine wesentliche Vereinfachung des Datentransfers durch eine Firewall bedingt. Die wesentlichen Sicherheitsmechanismen – Verschlüsselung der gesamten Kommunikation (Credentials und Nutzdaten) sowie Authentifikation – stellt dabei SSH zur Verfügung. Zu diesen kryptografischen Funktionen gibt es auch eine ausführliche Spezifikation des BSI in Form der technischen Richtlinie TR-02102[9].

SFTP wurde allerdings nie offiziell als Internet-Standard definiert. Demgegenüber wurde FTPS im RFC 4217 spezifiziert. Das – im Gegensatz zu SFTP – native FTP-Protokoll wird dabei um eine Verschlüsselung und Authentifizierung auf Basis von TLS ergänzt. Da, wie bereits erwähnt, FTP mindestens zwei Verbindungen benötigt, ist diese Lösung nicht sehr „Firewall-freundlich“, denn zum Datentransfer müssen mehrere Ports geöffnet werden. Auch werden in verschiedenen Implementierungen nur die Authentifizierungsdaten verschlüsselt, nicht jedoch die In-

8 https://www.allianz-fuer-cybersicherheit.de/dok/6649706
9 TR-02102, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html p. 70f.

haltsdaten(!). Je nach Konfiguration von Clients und Servern kann es dadurch zu Inkompatibilitäten kommen, die einen Verbindungsaufbau sogar verhindern. Von der Handhabbarkeit ist hier SFTP in jedem Fall zu bevorzugen.

Neben FTPS und SFTP stellt auch SCP eine sichere Alternative zum unverschlüsselten FTP dar. Auch hierzu sei auf die o. g. TR-02102 verwiesen.

Managed Devices

SNMP (**Simple Network Management Protocol**) ist ein verbreitetes Protokoll, um netzwerkverbundene Geräte zentral zu überwachen und zu steuern. Aktuell ist insbesondere SNMPv2 bzw. genauer gesagt SNMPv2c verbreitet. Problematisch hieran ist jedoch, dass SNMP bis einschließlich SNMPv2(c) keine Verschlüsselung bietet, d. h. sämtliche Daten werden menschenlesbar im Klartext übertragen. Zudem kann praktisch jeder Teilnehmer im Netzwerk Systeminformationen auslesen und somit mitunter kritische Informationen erhalten. Da SNMPv1 und SNMPv2 auf UDP aufbauen, sind diese zustandslos, was zudem die Anfälligkeit für IP Spoofing erhöht.

Mit SNMPv3 (Version 3) wurden Funktionen, wie Verschlüsselung und eine verbesserte Authentisierung eingeführt. Aus diesem Grund ist zu empfehlen, prinzipiell SNMPv3 zu implementieren und dieses möglichst in der Standardkonfiguration zu aktivieren. Hinsichtlich der Kompatibilität zu bestehenden Systemen kann auch SNMPv2(c) zusätzlich implementiert werden, welches dann allerdings durch den Betreiber zu aktivieren sein sollte.

Zu beachten ist, dass auch bei SNMPv3 gewisse Restrisiken verbleiben. Insbesondere Brute Force- und Wörterbuch-Angriffe auf die Authentisierung sind möglich. Daher ist es sinnvoll, einen geeigneten Detektionsmechanismus für solche Angriffe zu integrieren. Zusätzlich sollte ein schreibender Zugriff nur wenn nötig implementiert werden bzw. sollte dieser deaktivierbar sein.

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.