Bewährtes Wissen in neuen Spezifikationen zu Industrial Security

Komponenten der funktionalen Sicherheit schützen das Leben und die Gesundheit von Personen, etwa indem sie den Zugang zu gefährlichen Bereichen von Maschinen und Anlagen verhindern. Wichtig ist, dass auch Manipulationen von außen die Sicherheit nicht beeinträchtigen. Dazu muss der Stand der Technik konsequent umgesetzt werden und Hersteller und Betreiber müssen im Falle von Sicherheitslücken angemessen darauf reagieren.

Damit Sicherheitsfunktionen von Steuerungen zuverlässig funktionieren können, muss auch die Steuerung selbst sicher sein – geschützt also vor Ausfall und Manipulation. Die steigende Frequenz neuer Katastrophenmeldungen im Bereich Industrial Security wirkt erschreckend. Doch es gibt Grund zur Hoffnung, denn fast alle Sicherheitslücken können nach dem Stand der Technik eigentlich sehr leicht vermieden werden, wie folgendes typische Beispiel zeigt.

Bereits 1883 stellte Auguste Kerckhoffs sechs Grundvoraussetzungen für eine vertrauliche Kommunikation auf. Die zweite lautete „Das System darf keine Geheimhaltung erfordern und muss ohne Nachteil in die Hände des Feindes fallen können“. Diese Schrift kannte Guglielmo Marconi offensichtlich nicht. Seine Telegraphie zur vertraulichen Kommunikation erforderte, dass niemand in Besitz eines der Geräte kommt oder eines nachbaut und auf die gleiche Frequenz einstellt. Nevil Maskelyne machte 1903 auf das Problem aufmerksam, indem er während Marconis Vorführung unflätige Nachrichten dazwischen morste, und gilt dadurch als einer der ersten Hacker. Obschon die sichere Verschlüsselung mit kryptographischen Methoden lange bekannt ist, findet sich der gleiche Designfehler auch heute noch etwa in Funksteuerungen für Ampelsysteme[1] oder Industriekranen[2].

Es fehlt an einheitlicher Definition der Begriffe

Der Navigator für Normen mit Bezug zu Security von der Universität Bremen[3] hat aktuell rund 800 Normen und über 2000 Treffer zu Rechtsvorschriften in einer Datenbank erfasst. Problematisch ist, dass die Dokumente unterschiedliche Begriffe verwenden und zum Teil nicht eindeutig definieren. Während manche Dokumente umfassend von Security oder Informationssicherheit handeln, erfinden andere neue Begriffe als Kofferwort aus „Cyber“ und einem weiteren Wort. Diese neu geschaffenen Wörter müssen im Dokument genau definiert werden, da sie für sich keine eindeutige Bedeutung haben. Mal ist „Cybersicherheit“ eine Tätigkeit, mal ist es eine Maßnahme gegen Angriffe aus dem Internet, ein anderes Mal ein Zustand, bei dem das Produkt vor Angriffen über Funk geschützt ist.

Besser als neue Wörter zu erzeugen ist es, mit den eindeutigen Begriffen Informationssicherheit oder Security zu arbeiten. Muss der Bedeutungsumfang etwa auf Angriffe über Funk reduziert werden, sollte die Einschränkung klar benannt werden. Einen anderen sehr eleganten Weg hat die EU-Maschinenverordnung gewählt, indem sie in Anhang III 1.1.9 einen „Schutz gegen Korrumpierung“ fordert und in diesem Punkt auch deutlicher ist als die bisherige EU-Maschinenrichtlinie. Dabei fokussiert sie sich auf das Schutzziel, dass etwa bei Fernzugriff keine gefährlichen Situationen entstehen dürfen und lässt offen, wodurch die Korrumpierung im Detail hervorgerufen wird.

Schnelle Kommunikation ist entscheidend

Eine schnelle und effektive Kommunikation ist der Schlüssel zur angemessenen Reaktion auf Sicherheitslücken. Wie schlecht es jedoch um die Kommunikation bestellt ist, zeigte sich im Dezember 2021, als eine Sicherheitslücke in der Softwarebibliothek Log4J Schlagzeilen machte. Diese Softwarebibliothek ist nicht nur Bestandteil vieler Serverdienste, sondern auch vieler Industriekomponenten. Während einerseits Vorwürfe laut wurden, dass die Bibliothek falsch eingesetzt wurde und die Sicherheitsprobleme durch Lesen der Dokumentation verhindert worden wären, rätselten gleichzeitig viele Hersteller, ob sie von Sicherheitslücken betroffen sind. Nicht selten brauchten Hersteller viele Monate, bis sie wussten, ob ihre Produkte betroffen sind.

Zusammengefasst fehlte es an

- einem Notfallkontakt für Security innerhalb des Unternehmens,
- einem einheitlichen Format für Handlungsempfehlungen und
- einem Standard, nach dem Hersteller auch mitteilen können, dass ein bestimmtes Produkt nicht von einer Sicherheitslücke betroffen ist.

Der Mangel an einheitlichen Informationen und Schnittstellen wird durch einen Satz offener Spezifikationen behoben, die von verschiedenen Zusammenschlüssen von Unternehmen, Behörden und Organisationen erarbeitet wurden und die jedes Unternehmen ab sofort umsetzen kann (siehe Tabelle). Ein Notfallkontakt nach der IETF-Spezifikation RFC 9116 wird in einer einfachen security.txt-Datei auf der Webseite hinterlegt[4]. Darin kann ein Hersteller auch auf seine Liste der Handlungsempfehlungen (CSAF) verweisen. Jedes Hardware- und Softwareprodukt bekommt eine weltweit eindeutige Identifikation (CPE), damit die Internationalen Warnmeldungen (CVE) automatisch den exakten Produkten und Versionen zugeordnet werden können. Die Kritikalität der Sicherheitslücke wird durch einen weltweit einheitlichen Index (CVSS) so gut es eben geht eingestuft. Anhand der offenen Spezifikation SPDX kann zu jedem Projekt maschinenlesbar dokumentiert werden, welche Bibliotheken verwendet wurden. Auf Betreiberseite kann dann ein Programm zu allen Produkten regelmäßig abfragen, ob Sicherheitswarnungen vorliegen und die Handlungsempfehlungen anzeigen.

Einige große Unternehmen setzen bereits auf diese Spezifikationen. Entscheidend ist nun, dass auch alle anderen Unternehmen schnell folgen, damit die Information zu Sicherheitsproblemen schnell und kostensparend erfolgt.

Als ersten Schritt sollten Unternehmen jetzt zumindest die Erreichbarkeit bei Sicherheitsvorfällen sicherstellen und einen Notfallkontakt bekannt machen. Mit der Anleitung auf https://cert.dguv.de kann das in wenigen Minuten umgesetzt werden.

Jonas Stein

Leiter des Prüflabors für Industrial Security und Leiter des Arbeitskreises Security der DGUV

Jonas.Stein@dguv.de

Offene Spezifikationen zur Informationssicherheit

Eingangsinformation	Gepflegt durch	Spezifikation
Eigener Notfallkontakt	Hersteller, Betreiber	„security.txt“ RFC 9116
Produktkennung / ID (Herstellername, Produktname, Version, Sprachausführung, ...)	Hersteller	CPE
Softwareliste (Software Bill of Materials – SBOM)	Hersteller	SPDX
Warnmeldung zur Sicherheitslücke	CVE-Nummerierungsstellen	CVE
Security Advisory (Handlungsempfehlung zur CVE)	Hersteller	CSAF
Eigenschaften zur Bewertung der Kritikalität	Hersteller	CVSS

Satz offener Spezifikationen, die gemeinsam einen entscheidenden Beitrag zur Industrial Security liefern werden. Sie werden die Kommunikation zu Sicherheitslücken in den kommenden Jahren auf die dringend erforderliche Geschwindigkeit beschleunigen.

1 ARD-Reportage 2021, https://ardmediathek.de „Hacker schalten Ampeln in Hannover auf Grün“
2 Andersen et al, 2019 “A Security Analysis of Radio Remote Controllers for Industrial Applications”, https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
3 https://cybersecurity-navigator.de
4 Kritische Sicherheitslücken an Maschinen und Anlagen und Kontaktstandard security.txt; https://cert.dguv.de