Fernwartung von Industriesteuerungen

Key Facts

- Die Fernwartung einer Industriesteuerung kann als Einfallstor für Hackerangriffe genutzt werden
- Eine rückwirkungsfreie Trennung zwischen sicherheitsrelevanten Komponenten und der nicht sicherheitsrelevanten Steuerung wie in Abbildung 4 dargestellt, kann daher die sichere Fernwartung deutlich vereinfachen und langfristig Kosten senken
- Sichere und praxisgerechte Zugangsberechtigungen sind die Grundvoraussetzung für eine sichere Fernwartung

Autor

↗ **Jonas Stein**

Der Artikel zeigt an Beispielen aus der Praxis, warum die Fernwartung von Industriesteuerungen technisch und organisatorisch eine große Herausforderung darstellt und welche Lösungsansätze dabei helfen können, eine sichere Fernwartung in Betrieben zu implementieren.

Probleme und Lösungsansätze an einem Beispiel beleuchtet

Der rasant zunehmenden Vernetzung von Steuerungen steht eine zunehmende Frequenz erfolgreicher Angriffe gegenüber. Das wirkt sich auch sofort auf die Sicherheit und Gesundheit bei der Arbeit aus, wie Angriffe etwa auf einen Hochofen im Ruhrgebiet oder eine petrochemische Anlage zeigen.[1] Betroffen sind jedoch nicht nur Anlagen der Schwerindustrie und der chemischen Industrie. Selbst unscheinbare Anlagen wie Raumluftsysteme in Bürokomplexen sind mittlerweile vernetzt. Sie können mit böswilliger Konfiguration Algen und Schimmelsporen in der Luft verteilen. Es ist sogar denkbar, dass die vernetzte Warmwassertherme einer Kindertageseinrichtung nach einem Angriff Kinder mit zu heißem Wasser am Waschbecken verletzt.

Die Techniken, mit denen die Fernwartung einer Industriesteuerung zu ermöglichen sind, sind extrem unterschiedlich und müssen genau an die jeweilige Situation angepasst werden. Zur Veranschaulichung sollen in Abbildung 1 einige kritische Punkte an einer minimalistischen Beispielanlage dargestellt werden.

Im Negativ-Beispiel aus Abbildung 1 wird eine programmierbare Sicherheitssteue-

Bildquelle: Jonas Stein/IFA

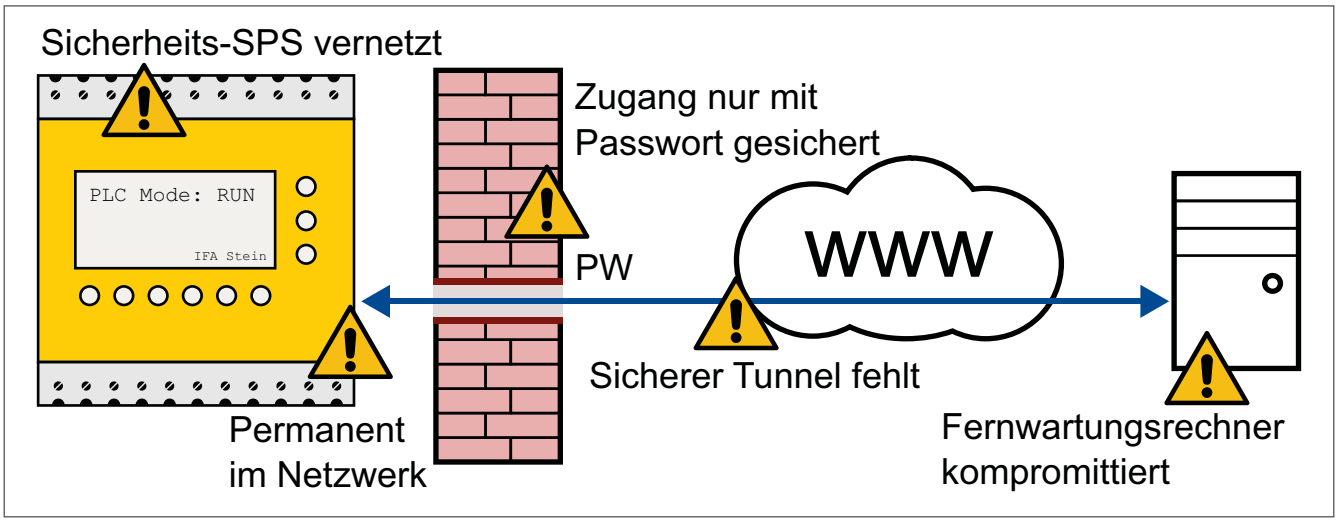


Abbildung 1: Exemplarisch werden einige typische Schwachstellen einer Industriesteuerung mit Fernwartungslösung dargestellt. Das System besteht aus einer programmierbaren Sicherheitssteuerung, die über einen Netzwerkanschluss verfügt und über das Internet zur Fernwartung über einen fremden Rechner erreichbar ist.

rung dauerhaft über einen Netzwerkanschluss bereitgestellt. Dabei sind Anforderungen aus dem Produktsicherheitsgesetz (ProdSG) zu beachten, woraus sich eine Vielzahl vermeidbarer Probleme ergeben, auf die im Folgenden eingegangen wird.

Wesentliche Änderung im Produktsicherheitsgesetz

Die Bereitstellung von Maschinen auf dem Markt wird im Produktsicherheitsgesetz[2] geregelt. Zur Veränderung an gebrauchten Produkten stellt das Interpretationspapier des Bundesministeriums für Arbeit und Gesundheit (BMAS) über die „Wesentliche Veränderung von Maschinen" fest: Nach dem „ProdSG ist ein gebrauchtes Produkt, das gegenüber seinem ursprünglichen Zustand **wesentlich** verändert wird, als neues Produkt anzusehen".[3]

Sollen bei einer Fernwartung Eigenschaften der Anlage verändert werden, muss geprüft werden, ob eine wesentliche Änderung vorliegt. Das Interpretationspapier des BMAS unterscheidet dabei die folgenden drei möglichen Fälle:

1. Die Maschine ist auch nach der Veränderung ohne zusätzliche Schutzmaßnahmen sicher. Es liegt **keine wesentliche Veränderung** vor.
2. Die Maschine ist nach der Veränderung ohne zusätzliche Schutzmaßnahmen nicht mehr sicher. Die neue Gefährdung oder das erhöhte Risiko können durch einfache Schutzeinrichtungen beseitigt oder zumindest hinreichend minimiert werden. Es liegt **keine wesentliche Veränderung** vor.
3. Die Maschine ist nach der Veränderung ohne zusätzliche Schutzmaßnahmen nicht mehr sicher und eine ausreichende Risikominderung kann nicht durch einfache Schutzeinrichtungen erreicht werden. Es liegt eine **wesentliche Veränderung** vor.

Übertragen auf eine Veränderung der Software durch eine Fernwartung kann a priori nicht angenommen werden, dass die Veränderung keine Auswirkungen auf die Sicherheit hat.

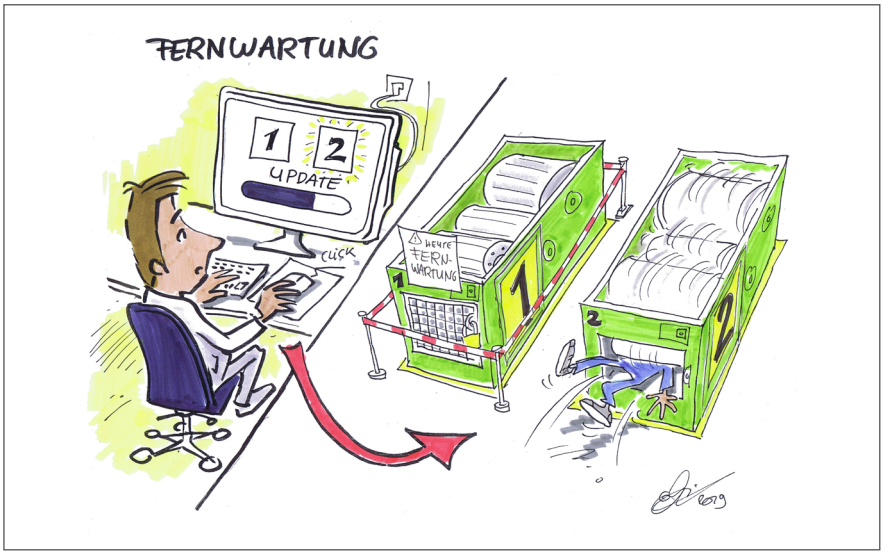
Nicht selten verursacht ein Bugfix[4] neue Probleme. So wurden etwa kürzlich in einer der am weitesten verbreiteten Softwarebibliotheken aus dem Bereich der Embedded-Systeme Fehler behoben[5] und dadurch ein noch gravierenderer erzeugt[6].

Eine rückwirkungsfreie Trennung zwischen sicherheitsrelevanten Komponenten und der nicht sicherheitsrelevanten Steuerung wie in Abbildung 4 dargestellt kann daher die sichere Fernwartung deutlich vereinfachen und langfristig Kosten senken.

Offene Schnittstellen

Damit eine Fernwartung möglich ist, muss eine Schnittstelle für die Verbindung bereitstehen. Es sind jedoch Sicherheitslücken bekannt, bei denen alleine die Erreichbarkeit der Schnittstelle schon für einen erfolgreichen Angriff genügt. Es sind keine Benutzernamen oder Anmeldedaten notwendig. Ein solches Beispiel ist der als Ripple20[7] bezeichnete Satz aus 19 kritischen Sicherheitslücken in einer bestimmten Softwarebibliothek, die in vielen Industriesteuerungen und anderen Netzwerkkomponenten eingesetzt wird. Das Nachrichtenmagazin Wired schätzt, dass weltweit rund 100 Millionen Steuerungen davon betroffen sind.[8] Weil weder die Hersteller noch die Betreiber oder ihre Dienstleister betroffene Steuerungen schnell genug lokalisieren und schützen können, ist es für die Sicherheit entscheidend, eine Verbindung nicht dauerhaft bestehen zu lassen, sondern zeitlich auf das absolut notwendige Minimum zu begrenzen. Die Verbindung sollte immer erst bei Bedarf hergestellt werden. Eine automatische Trennung nach einer vorgegebenen Zeit verhindert zusätzlich, dass eine Schnittstelle dauerhaft exponiert bleibt, falls die geplante Trennung ausbleibt. Der Angriff TRISIS[9] auf eine Sicherheitssteuerung mit dem Ziel, eine petrochemische Anlage zu zerstören, war möglich, weil die Steuerung länger als notwendig die Schnittstelle offen gehalten hat.

Mit der zunehmenden Anzahl fernwartbarer Steuerungen steigt auch die Wahrscheinlichkeit einer Gefahr bringenden Verwechslung. Der Verwechslungsgefahr kann durch einen zweiten Faktor der Authentifizierung entgegengewirkt werden, der an die Freigabe einer Maschine zur Wartung gekoppelt ist. Zum Beispiel könnte beim lokalen Freischalten der Schnittstelle im Display der Maschine eine Nummer erscheinen, die telefonisch übermittelt wird und die in die Anmeldung einfließt.



Bildquelle: Michael Hüter

Abbildung 2: Bei der Fernwartung von Maschinen und Anlagen muss eine Verwechslung unbedingt verhindert werden. Technische Lösungen, die eine Verwechslung verhindern, können dazu bereits mit der lokalen Freigabe kombiniert werden.

Zugangsberechtigung

Eine Grundvoraussetzung für eine sichere Fernwartung ist die sichere und praxisgerechte Zugangsberechtigung. Was an einem Bürorechner eine Herausforderung ist, wird im Bereich von Industriesteuerungen nicht einfacher.

Während die Daten eines Desktoprechners bei einer verloren gegangenen Zugangskennung spätestens durch die Wiederherstellung einer Datensicherung wieder verfügbar sind, kann der Verlust der Zugangsdaten einer Industriesteuerung zu langen Produktionsunterbrechungen mit enormen Verlusten führen. Viele Anlagen benötigen für den Betrieb eine zwei bis dreistellige Zahl sehr unterschiedlicher Steuerungen. Analog zur Manipulation an Maschinen fördert ein praxisuntaugliches, heterogenes Netzwerk aus Steuerungen den Manipulationsanreiz. In der Folge findet die Empfehlung, für jede Steuerung ein individuelles, starkes Passwort zu vergeben, keine Anwendung. Biometrische Authentifizierungen über den Fingerabdruck, eine Gesichtserkennung oder einen Irisscan sind im Industrieumfeld oft ungeeignet. Zum einen muss sich oft viele Jahre niemand an der Steuerung anmelden, zum anderen sinkt die Erkennungsrate in rauen Industrieumgebungen deutlich. Sicherheitsforschende berichten, wie sie aus vielen Porträts ein Bild berechnen, das sich als Generalschlüssel für Angriffe auf die Gesichtserkennung eignet.[10]

Eine Authentifizierung durch kryptografische Hardware lässt sich dagegen deutlich leichter prüfen und zertifizieren als die deutlich komplexeren biometrischen Verfahren. Diese Hardware – oft auch Tokens genannt – sieht oft wie USB-Sticks aus und ist in der Anwendung so einfach wie ein klassischer Schlüssel. Damit sind kryptografische Tokens langfristig eine vielversprechende Alternative zu dem weniger sicheren und unpraktischen Passwort.

Netzwerkkomponenten

Filterregeln in Firewalls verhindern, dass mehr Datenpakete als notwendig in den jeweils hinterlegten Routen passieren können. Im Zusammenhang mit der Fernwartung müssen sie durchtunnelt werden oder eine bestimmte Paketroute zur Fernwartung erlauben. Sie haben zwei besonders kritische Schwachstellen. Sie können selbst kritische Sicherheitslücken mitbringen, die einen Angriff erst ermöglichen. Die Sicherheitswarnung[11] beschreibt, wie ohne Anmeldung ein beliebiger Code auf einer Firewall ausgeführt werden kann. Ein weiteres Problem ist, dass die korrekte Funktion einer Firewall oft nicht überwacht wird. Falls die Filter dann nach einem Update oder einer Konfigurationsänderung durch einen Fehler nicht mehr greifen, ist das Firmennetz unbemerkt exponiert.

Verschlüsselungssysteme für Netzwerkverbindungen werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Geheimschutz zertifiziert.[12] Man kann nun leicht vermuten, dass eine Zertifizierung für die höchste Geheimhaltungsstufe „STRENG GEHEIM“ auch den Datenverkehr für eine Fernwartung an einer Maschine, die Personen verletzen kann, gut schützen wird. Billiger und riskanter wäre es, eine Fernwartung nicht nach dem aktuellen Stand der Wissenschaft zu schützen, sondern nur die jeweils für die Anwendung minimal notwendigen Maßnahmen umzusetzen. Genau hier unterscheidet sich der Handlungsspielraum der Safety und der Security. Ursachen für einen Unfall werden unabhängig von der Konstruktion einer Schutzeinrichtung immer in der gleichen statistischen Verteilung eintreten. Werden jedoch bestimmte Security-Maßnahmen nicht umgesetzt, werden Angriffe auf diese Schwachstellen stark zunehmen.

Fernwartungsrechner

Eine sichere Fernwartung ist nur möglich, wenn den Kommandos vom Fernwartungsrechner vertraut werden kann. Bei den Angriffen STUXNET und TRISIS war ein kompromittierter Rechner mit der Steuerung verbunden. Weil Fernwartungsrechner in der Praxis wie in Abbildung 3 gezeigt selten isoliert von anderen Netzen sind, stellt dies einen sehr einfachen und häufigen Angriffspfad dar.

Nach der IEC 61508 oder ISO 13849 könnte der Fernwartungsrechner als Bestandteil der Anlage betrachtet werden. Wesent-

Bildquelle: Jonas Stein/IFA

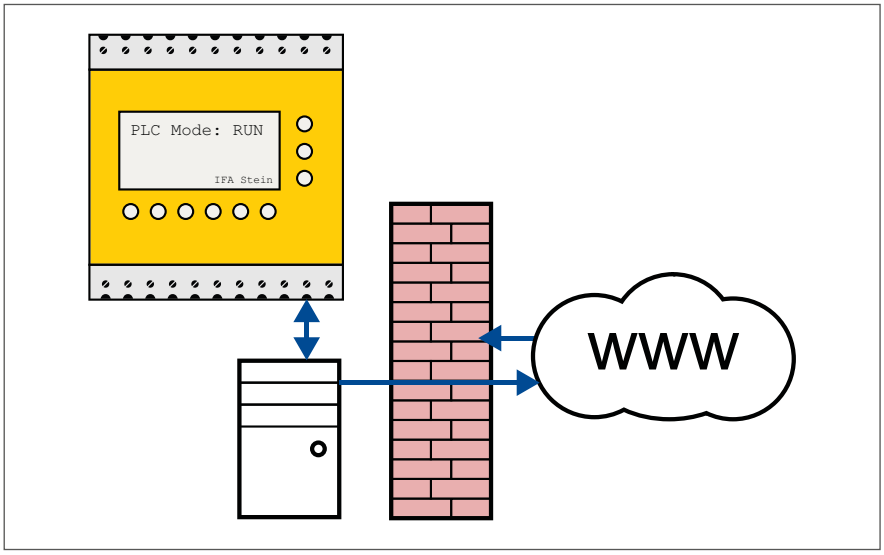
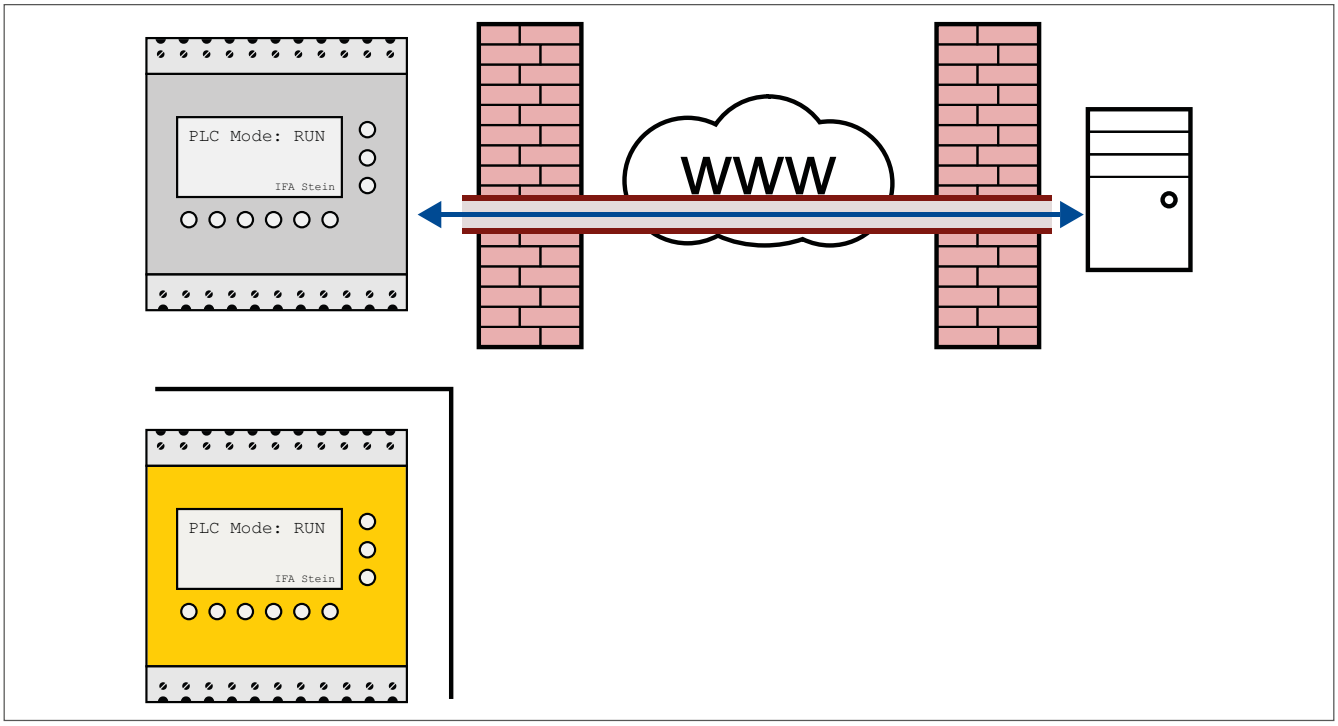


Abbildung 3: Die Sicherheitssteuerung ist hier mit einem Rechner verbunden. Beide befinden sich innerhalb einer demilitarisierten Zone und sind durch eine Firewall geschützt. Der Rechner erhielt jedoch über eine E-Mail eine Schadsoftware, mit der ein Tunnel durch die Firewall geöffnet werden konnte. Über den kompromittierten Rechner kann nun die Steuerung leicht angegriffen werden.

lich einfacher ist es jedoch, ihn bezogen auf die Sicherheitssteuerung wie in der Abbildung 4 gezeigt rückwirkungsfrei zu verbinden. Damit Betriebe für Warnungen erreichbar sind, wurde ein Standard verabschiedet, nach dem jeder Betrieb kostenlos einen Notfallkontakt auf der eigenen Webseite in einem international standardisierten Pfad hinterlegen kann.[13] Viele Betriebe haben diesen kostenlosen Standard bereits umgesetzt.[14]

Fazit

Eine unüberlegte Vernetzung zur Fernwartung von Maschinen und Anlagen kann nicht nur Wirtschaftsgütern schaden, sondern stellt auch eine reale Bedrohung für die Gesundheit dar. Damit die Vorteile einer Fernwartung zur Geltung kommen können, muss diese sicher gestaltet und gepflegt werden. Die aufgeführten Beispiele und Lösungsansätze zeigen, dass es zwar viele Fallen gibt, aber Lösungen vorhanden sind. Sie helfen, mögliche Schwachstellen in vorhandenen Lösungen zu erkennen. Das Institut für Arbeitsschutz der DGUV (IFA) unterstützt Unfallversicherungsträger und Hersteller von Produkten bei der Umsetzung der Anforderungen an die Security. Es will das Bewusstsein für und den Umgang mit Security-Fragen nachhaltig verbessern und für akute Sicherheitsprobleme in Betrieben sensibilisieren.



Bildquelle: Jonas Stein/IFA

Abbildung 4: Die Steuerung der Maschine wurde hier rückwirkungsfrei von der Sicherheitssteuerung in einer Fernwartungslösung integriert. Die Anlage wurde so konstruiert, dass Produktionsdaten ausgelesen und Rezepte angepasst werden können, ohne dass das Kriterium der wesentlichen Änderung erfüllt wird. Ein sicherer Tunnel verbindet die Steuerung mit einem Fernwartungsrechner, der keine Verbindung zu anderen Netzen hat.

Fußnoten

[1] www.dragos.com/wp-content/uploads/TRISIS-01.pdf, abgerufen am 14.08.2021
[2] Produktsicherheitsgesetz, www.gesetze-im-internet.de/prodsg_2021, abgerufen am 14.08.2021
[3] Bundesministerium für Arbeit und Soziales, Produktsicherheitsgesetz/9. ProdSV (Maschinenverordnung), Interpretationspapier zum Thema „Wesentliche Veränderung von Maschinen“ (Bek. des BMAS vom 09.04.2015 – IIIb5-39607-3 – im GMBl 2015, Nr. 10, S. 183–186)
[4] Ein Bugfix bezeichnet in der Regel eine Änderung im Quelltext mit dem Ziel, einen Softwarefehler (englisch: Bug) zu beheben.
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33574, abgerufen am 14.08.2021
[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38604, abgerufen am 14.08.2021
[7] www.jsof-tech.com/disclosures/ripple20/#ripple-disclosure, abgerufen am 14.08.2021
[8] www.wired.com/story/ripple20-iot-vulnerabilities, abgerufen am 14.08.2021
[9] www.dragos.com/wp-content/uploads/TRISIS-01.pdf, abgerufen am 14.08.2021
[10] www.heise.de/news/Forscher-entdecken-Generalschluessel-fuer-Systeme-zur-Gesichtserkennung-6156605.html, abgerufen am 14.08.2021
[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3331, abgerufen am 14.08.2021
[12] www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Liste-zugelassener-Produkte/liste-zugelassener-produkte_node.html, abgerufen am 14.08.2021
[13] https://securitytxt.org, abgerufen am 14.08.2021
[14] www.google.com/.well-known/security.txt, abgerufen am 14.08.2021