80168

Fachzeitschrift für Prävention, Rehabilitation und Entschädigung

Ausgabe 12 • 2019

DGUV Forum

Herausforderung Digitalisierung

Aus der Forschung
Veranstaltungen und deren Wirksamkeit

In eigener Sache
DGUV Forum geht online

DGUV
Deutsche Gesetzliche Unfallversicherung
Spitzenverband

Industrial Security

Angriffe auf vernetzte Industriesteuerungen

Die Sicherheitsfunktionen an Maschinen und Anlagen werden oft mithilfe von programmierbaren elektronischen Systemen realisiert. Zufälliges oder mit Absicht herbeigeführtes Fehlverhalten solcher Systeme stellt eine Gefahr für den Arbeitsschutz dar.

Aktuelle Lage der Sicherheit für den Arbeitsschutz

Damit Sicherheitsfunktionen von Systemen zuverlässig funktionieren, müssen diese vor Ausfall und Manipulation besonders geschützt sein. So kann eine Manipulation an der Steuerung in einem Chemiewerk zur Zerstörung des Werks führen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet eine zunehmende Anzahl solcher Angriffe. Sowohl die Herkunft als auch die genauen Absichten sind oft nicht eindeutig rekonstruierbar. Häufige Gründe für solche Angriffe sind Erpressungen oder die Absicht, einem bestimmten Wirtschaftszweig regional zu schaden. Manchmal ist jedoch kein wirtschaftlicher Zusammenhang erkennbar, oder ein System wurde willkürlich ausgewählt.

Früher war es üblich, dass Steuerungen in einem Schaltschrank ohne Verbindung zur Außenwelt eingebaut waren. Seit etwa einem Jahrzehnt kann man beobachten, dass Steuerungen selbst dann vernetzt werden, wenn die Anwenderinnen und Anwender die Vernetzung nicht nutzen. Die vernetzten Steuerungen werden dadurch potenziellen Angriffen unnötig ausgesetzt.

Die Gefahr bringende Sabotage einer Anlage erforderte früher, dass die angreifende Person zur Anlage reist, sich Zugang verschafft und nach der Sabotage möglichst unentdeckt wieder verschwindet. Jeder Angriffsversuch war mit sehr hohem Zeit- und Kostenaufwand verbunden. Der Aufwand für zwei Angriffe auf verschiedene Anlagen war daher auch etwa zweimal so hoch.

Dagegen unterscheidet sich der Aufwand für zwei oder zweitausend Angriffe auf hoch vernetzte Steuerungen kaum. Denn sobald ein Angriff auf eine Sicherheitslücke vorbereitet ist, kann er praktisch gleichzeitig auf alle vergleichbaren Systeme an jedem Ort der Welt angewendet werden.

Diese Eigenschaften machen Angriffe auf vernetzte Systeme hoch attraktiv. Tabelle 1 zeigt Meilensteine in der Entwicklung von Schadsoftware für Angriffe auf Industriesteuerungen. Die Schadsoftware Stuxnet wurde im Jahr 2010 bekannt[1] [2]. Es folgten Modifikationen von Stuxnet, aber auch Neuentwicklungen, die 2017 erstmals gezielt für sicherheitsrelevante Steuerungen programmiert wurden.

Für einen Angriff auf eine Steuerung ist es meist nicht notwendig, extra eine Schadsoftware zu entwickeln. Wie einfach Angriffe auf Steuerungen sind, wurde erst kürzlich für Insulinpumpen[3], Herzschrittmacher[4] und Industriekrane[5] demonstriert. Dass Angriffsmöglichkeiten auf Steuerungen auch tatsächlich umgesetzt werden und eine reale Bedrohung darstellen, zeigte sich, als sich 2014 der Hochofen in einem deutschen Stahlwerk durch einen Angriff nicht mehr kontrolliert herunterfahren ließ.[6]

Was unterscheidet Office-IT von vernetzten Industriesteuerungen?

Im Bereich der Office-IT ist die Bedrohung sehr präsent, aber das Schadensausmaß ist vergleichsweise gering. Die wesentlichen Unterschiede zwischen Büronetzen und industriellen Steuerungsnetzwerken in Tabelle 2 heben den Kern der Herausforderung hervor: Ein hohes potenzielles Schadensausmaß bis zur Zerstörung der Anlage und Personenschäden stehen hohen Anforderungen an die Verfügbarkeit gegenüber.

> **Sicherheit**
>
> Im Englischen kann der Begriff Sicherheit feiner unterschieden werden: Die Sicherheit vor nicht absichtlich herbeigeführten Gefährdungen wird mit Safety beschrieben. Dagegen wird die Sicherheit vor absichtlich herbeigeführten Gefährdungen mit Security bezeichnet.

Sicherheitsexperte Bruce Schneier kritisiert, dass die Softwarequalität in aller Regel so schlecht ist, dass wir uns über die Jahre bereits an regelmäßige Fehler und Systemabstürze gewöhnt haben.[7] Angreifende nutzen diese bereits vorhandenen Softwarefehler.

Einfache Maßnahmen zur Erschwerung der Gefahr bringender Angriffe

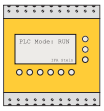
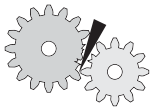
Derzeit ist die Anmeldung mit einem Benutzernamen und einem Passwort bei Steuerungen am weitetesten verbreitet. Daraus ergeben sich viele Probleme: Passwörter sind voreingestellt und werden nicht geändert. Der Sicherheitsforscher Troy Hunt hat bereits mehr Zugangsdaten öffentlich lesbar im Internet gefunden als Menschen auf der Erde leben.[8] Dies zeigt, wie wichtig es ist, nie das gleiche Passwort für verschiedene Anmeldungen zu verwenden. Bis andere Verfahren etwa mit kryptografischen Chipkarten verbreitet sind, kann durch ein starkes Passwort ein Angriff erschwert werden.

- Eine Überprüfung der eigenen Passwörter gehört somit zu den einfachen und preiswerten Maßnahmen, die alle umsetzen können. Bei manchen Industriesteuerungen sind die verfügbaren Zeichen und die Passwortlänge stark eingeschränkt, aber Passwortmanager

Autor

Jonas Stein
Institut für Arbeitsschutz der DGUV (IFA)
E-Mail: jonas.stein@dguv.de

Tabelle 1: Schadsoftware für Industriesteuerungen

Jahr der Veröffentlichung	Name	 Vorgesehen für Standard SPS	 Vorgesehen für Safety SPS	 Absicht: Produktionsstopp	 Absicht: Zerstörung
2010	Stuxnet	X		X	(X)
2010	Blackenergy[2]	X			
2014	Havex/Backdoor.Oldrea	X			
2015	Industroyer/Crashoverride	X		X	
2017	Trisis/Triton/Hatman		X	X	X

Quelle: IFA

Tabelle 2: Grundlegende Unterschiede erschweren die Absicherung von vernetzten Industriesteuerungen gegenüber Büronetzen deutlich.

Wesentliche Eigenschaften	Office-IT	Industriesteuerungen
Schadensausmaß	Im Wesentlichen rein wirtschaftlich	Neben wirtschaftlichen Schäden auch Gefahr für die Gesundheit bei der Arbeit möglich
Vertraulichkeit	Hohe Anforderungen an Vertraulichkeit	Vertraulichkeit steht nicht im Vordergrund
Verfügbarkeit	Kurze Unterbrechungen sind unkritisch, Back-ups können Zustand vor Angriff wieder herstellen	Unterbrechungen können teuer und gefährlich sein. Physischer Schaden ist möglich
Produktlebensdauer	Größenordnung 2 Jahre	Größenordnung 20 Jahre
Änderungen	Mehrere Wartungen und Änderungen pro Jahr	Eine Wartung oder Änderung nach mehreren Jahren
Automatische Reaktionen auf Unregelmäßigkeiten	Bei Auffälligkeiten im Netzwerk können Verbindungen getrennt werden.	Hohe Anforderung an die Verfügbarkeit schränkt automatische Reaktionen ein
Architekturen	Sehr homogen	Sehr heterogen
Verfügbarkeit von Fachleuten	Spezialwissen zu IT-Security notwendig, wenige Fachleute auf dem Arbeitsmarkt	Spezialwissen zu IT-Security und Maschinensicherheit notwendig, extrem wenige Fachleute auf dem Arbeitsmarkt

Quelle: IFA/DGU

können zufällige Passwörter generieren und diese verwalten.

- Die Konferenz der Präventionsleiterinnen und Präventionsleiter der DGUV hat die Gründung des Arbeitskreises Security beschlossen. Der Arbeitskreis wird sich mit der IT-Sicherheit in industriellen Netzwerken und möglichen Folgen für die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit befassen.
- Ein Prüfgrundsatz für Industriekomponenten wurde durch die Berufsgenossenschaftlichen Prüfstellen und das Institut für Arbeitsschutz der DGUV (IFA)[9] entwickelt. Siehe dazu „Prüfung und Zertifizierung der industriellen IT-Sicherheit“ in DGUV Forum 6/2019, Seite 20.

Fußnoten

[1] www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

[2] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[3] www.wired.com/story/medtronic-insulin-pump-hack-app/

[4] Ries, U.: Möchten Sie sterben? Malware gegen Herzschrittmacher lässt Hersteller kalt, heise 2018, https://heise.de/-4133625

[5] Andersson, J.; Balduzzi, M.; Hilt, S.; Lin, P.: Maggi, F.; Urano, A. und Vosseler, R.: A Security Analysis of Radio Remote Controllers for Industrial Applications, Trend Micro Research 2018.

[6] Bundesamt für Sicherheit in der Informationstechnik: Bericht zur Lage der IT-Sicherheit in Deutschland 2014.

[7] Schneier, B.: Click Here to Kill Everybody, Security and Survival in a Hyper-connected World, ISBN: 978-0-393-60888-5, September 2018.

[8] https://haveibeenpwned.com/

[9] https://dguv.de/ifa/security/