Bundesamt
für Sicherheit in der
Informationstechnik



**ANGRIFFSMETHODEN**

# Industrial Control System Security

## Top 10 Bedrohungen

Automatisierungs-, Prozesssteuerungs- und -leitsysteme – subsumiert unter dem Begriff *Industrial Control Systems* (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln – von der Stromerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zu Produktion, Verkehrsleittechnik und modernem Gebäudemanagement. Dabei wurden Aspekte der Cyber-Sicherheit in der Vergangenheit nachrangig behandelt oder gar vernachlässigt. Betreiber solcher Anlagen müssen sich angesichts zunehmender Vorfälle und Schwachstellen dringend dieser Thematik annehmen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit erheblichem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

## 1 Aktuelle Bedrohungslage

Im Rahmen seiner Analysen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS-Systeme derzeit ausgesetzt sind. Im Zuge der geplanten Fortschreibung dieser Top 10 sollen zudem Trends bzgl. der kritischsten Bedrohungen aufgezeigt werden. Die Rangordnung der Bedrohungen ergibt sich aus einer Betrachtung von Aspekten wie beispielsweise Täterkreis, der Verbreitung und Ausnutzbarkeit der Schwachstellen sowie der möglichen technischen und wirtschaftlichen Folgen eines Angriffs. Dabei wurden u. a. etablierte Vorfallsdatenbanken ausgewertet.

Nicht in diesen Top 10 enthalten sind weitere Bedrohungen, die derzeit als nachrangig zu den hier Dargestellten erachtet werden. Hierzu gehört z. B. der Einsatz von Smartphones zu Steuerungszwecken oder der Trend hin zu Cloud Computing. Gleichwohl sind solche und alle weiteren im konkreten Einzelfall relevanten Bedrohungen für die Absicherung im jeweiligen Anwendungsfall geeignet zu berücksichtigen. Darüber hinaus wird der Safety-Aspekt explizit nicht behandelt.

# 2 Top 10 Bedrohungen

| Nr. | Bedrohung | Erläuterung |
|---|---|---|
| 1 | Unberechtigte Nutzung von Fernwartungszugängen | Wartungszugänge sind bewusst geschaffene Öffnungen des ICS-Netzes nach außen, die häufig nicht hinreichend abgesichert sind. |
| 2 | Online-Angriffe über Office- / Enterprise-Netze | Office-IT ist i. d. R. auf vielen Wegen mit dem Internet verbunden. Meist bestehen auch Netzwerkverbindungen vom Office- ins ICS-Netz, sodass Angreifer über diesen Weg eindringen können. |
| 3 | Angriffe auf eingesetzte Standardkomponenten im ICS-Netz | IT-Standardkomponenten (commercial off-the-shelf, COTS), wie Betriebssysteme, Application Server oder Datenbanken, enthalten in der Regel Fehler und Schwachstellen, die von Angreifern ausgenutzt werden. Kommen diese Standardkomponenten auch im ICS-Netz zum Einsatz, so erhöht dies das Risiko eines erfolgreichen Angriffs auf die ICS-Systeme. |
| 4 | (D)DoS Angriffe | Durch (Distributed) Denial of Service Angriffe können Netzwerkverbindungen und benötigte Ressourcen beeinträchtigt und Systeme zum Absturz gebracht werden, z. B. um die Funktionsfähigkeit eines ICS zu stören. |
| 5 | Menschliches Fehlverhalten und Sabotage | Vorsätzliche Handlungen – ganz gleich ob durch interne oder externe Täter – sind eine massive Bedrohung für sämtliche Schutzziele. Daneben sind Fahrlässigkeit und menschliches Versagen eine große Bedrohung insbesondere bzgl. der Schutzziele Vertraulichkeit und Verfügbarkeit. |
| 6 | Einschleusen von Schadcode über Wechseldatenträger und externe Hardware | Der Einsatz von Wechseldatenträgern und mobilen IT-Komponenten externer Mitarbeiter stellt stets eine große Gefahr bzgl. Malware-Infektionen dar. Dieser Aspekt kam z. B. bei Stuxnet zum Tragen. |
| 7 | Lesen und Schreiben von Nachrichten im ICS-Netz | Da die meisten Steuerungskomponenten derzeit über Klartextprotokolle und somit ungeschützt kommunizieren, ist das Mitlesen und Einspielen von Steuerbefehlen oftmals ohne größeren Aufwand möglich. |
| 8 | Unberechtigter Zugriff auf Ressourcen | Insbesondere Innentäter oder Folgeangriffe nach einer Penetration von außen haben leichtes Spiel, wenn Dienste und Komponenten im Prozessnetz keine bzw. unsichere Methoden zur Authentisierung und Autorisierung implementieren. |
| 9 | Angriffe auf Netzwerkkomponenten | Netzwerkkomponenten können durch Angreifer manipuliert werden, um z. B. Man-in-the-Middle Angriffe durchzuführen oder um Sniffing zu erleichtern. |
| 10 | Technisches Fehlverhalten und höhere Gewalt | Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind immer möglich – Risiko und Schadenspotential können hier lediglich minimiert werden. |

# 3 Danksagung

Die Auflistung der Bedrohungen ist in enger Zusammenarbeit zwischen BSI und Vertretern der Wirtschaft entstanden. Besonderer Dank gilt: Michael Kasper (CASED), Ingo Jensen (E.ON Netz GmbH), Dr. Stephan Beirer (GAI NetConsult GmbH), Alfred Pohl (Hauni Maschinenbau AG), Jörn Maier (HiSolutions AG), Jonathan Pollet (Red Tiger Security), Siemens AG (Industry Sector), Steffen Zimmermann (VDMA), Adrian Hehl (VICCON Gmbh), Rolf Strehle (Voith GmbH), Dr. Peer Wichmann (WIBU-SYSTEMS AG).