Schwachstellen und Risiken

Der Sicherheitssoftwarehersteller *Kaspersky Lab* hat mit dem Internet verbundene industrielle Kontrollsysteme untersucht und bei vielen Schwachstellen entdeckt.

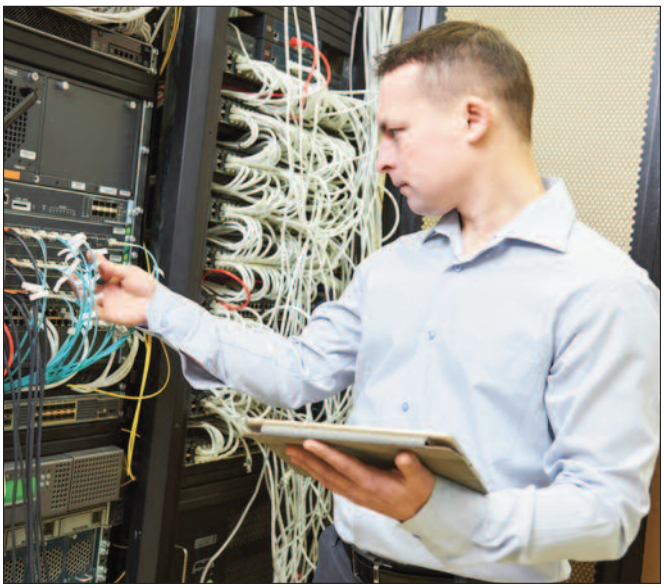
Sind industrielle Kontrollsysteme (Industrial Control Systems, ICS) mit dem Internet verbunden, besteht die Gefahr, dass sie von Kriminellen manipuliert werden, etwa indem sie ICS-Komponenten „fernsteuern". Das kann Schäden von Anlagenteilen zur Folge haben und ist eine Gefahr für die kritische Infrastruktur. Das Sicherheitssoftwareunternehmen *Kaspersky Lab* warnt vor möglichen Schwachstellen in diesen Systemen.

Beispiele für Angriffe auf ICS-Systeme sind die Attacken der Hackergruppe „Black-Energy-APT" auf ein Energieversorgungsunternehmen in der Ukraine, auf den Frederic-Chopin-Airport in Warschau 2015 und auf ein deutsches Stahlwerk 2014.

„Unsere Untersuchung zeigt: Je größer die Infrastruktur industrieller Kontrollsysteme ist, desto größer ist auch das Risiko empfindlicher Sicherheitslücken", sagt Andrey Suvorov von *Kaspersky Lab*. „Das liegt nicht an einzelnen Software- oder Hardware-Anbietern. ICS-Umgebungen sind eine Mischung aus verschiedenen miteinander verbundenen Komponenten. Viele davon sind an das Internet angeschlossen und werfen Sicherheitsfragen auf.

Es gibt keine hundertprozentige Garantie dafür, dass eine ICS-Installation nicht mindestens eine verwundbare Komponente enthält. Das wiederum bedeutet nicht, dass Fabriken, Kraftwerke oder Smart Citys nicht vor Cyber-Attacken geschützt werden können. Sicherheitsverantwortliche industrieller Anlagen sollten sich bewusst machen, dass schwachstellenbehaftete Komponenten innerhalb industrieller Systeme existieren. Mit unserer Untersuchung wollten wir auch das Bewusstsein einer interessierten Öffentlichkeit für dieses Thema schärfen."

Industrielle Kontrollsysteme, die mit dem Internet verbunden sind, können von Kriminellen manipuliert werden.



Sicherheitsaudits: Zur Identifizierung möglicher Schwachstellen sollten Experten beigezogen werden, die sich auf die Sicherheit für Industriebelange spezialisiert haben.

Industrielle Kontrollsysteme nutzen unsichere Internetverbindungsprotokolle, die Angreifern „Man-in-the-Middle"-Attacken ermöglichen. Dabei fängt ein Angreifer die Kommunikation zwischen zwei Systemen ab, um die übertragenen Daten mitzulesen und zu manipulieren.

Die von *Kaspersky* untersuchten industriellen Kontrollsysteme konnten großen Organisationen zugerechnet werden – aus den Bereichen Energie, Transport, Luft- und Raumfahrt, Industrie, öffentlicher Sektor oder Finanzen. 90 Prozent davon wiesen Schwachstellen auf, die aus der Ferne ausgenutzt werden konnten; 3,3 Prozent beinhalteten kritische Schwachstellen, die aus der Ferne manipuliert werden konnten.

Die verwundbarsten ICS-Komponenten waren Benutzerschnittstellen oder „Mensch-Maschine-Schnittstellen" (Human Machine Interfaces, HMI), elektronische Geräte und *SCADA-Systeme* (System Supervisory Control and Data Aquisition). Bei den für 2015 gefundenen Sicherheitslücken stufte *Kaspersky Lab* 49 Prozent als kritisch und 42 Prozent als mittelschwer ein.

Schutzmaßnahmen. Um industrielle Kontrollsysteme vor Cyber-Angriffen zu schützen, empfehlen die Experten von *Kaspersky Lab* folgende Sicherheitsmaßnahmen:

Sicherheitsaudits: Die schnellste Maßnahme zur Identifizierung und Schließung möglicher Schwachstellen ist das Beiziehen von Experten, die sich auf die Sicherheit für Industriebelange spezialisiert haben.

Externe „Intelligence": IT-Sicherheit hängt auch vom Wissen über potenzielle Angriffsvektoren ab. Die *Kaspersky Security Intelligence Services* bieten zum Beispiel Informationen zur Bedrohungslandschaft – auch für industrielle Systeme. Damit können Angriffe prognostiziert werden. Regelmäßige Integritätsprüfungen für Steuereinheiten sowie spezielles Sicherheits-Netzwerk-Monitoring minimieren das Risiko von Angriffen. *Siegbert Lattacher*

Fotos: Kadmy/Fotolia, Zapp2Photo/Fotolia