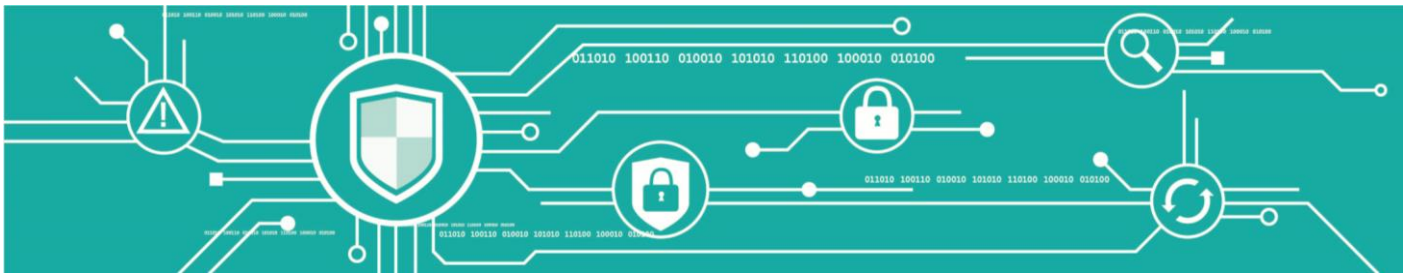


# Hacker-Attacke auf eine Wasserversorgung in der Innerschweiz

Diverse Medien berichteten im Dezember 2018 ausgiebig über eine Hacker-Attacke auf eine Wasserversorgung in der Innerschweiz. Diese Meldungen wurden von vielen Wasserversorgungsbetreibern mit grossem Interesse verfolgt und führten teilweise auch zu Verunsicherungen. Fakt ist, dass die Anzahl der Cyberbedrohungen zunimmt. Cyberkriminelle verwenden immer raffiniertere Angriffsmethoden und nutzen neue Sicherheitslücken schneller aus. Die Sicherheit für kritische Infrastrukturen bleibt eine Herausforderung und deren Betreiber sollten und müssen sich intensiv mit den Anforderungen, welche heute sowie in Zukunft an die IT-Sicherheit gestellt werden, auseinandersetzen.

## Um was geht es?

Die Medien berichteten im Dezember 2018 über einen Hacker-Angriff auf die IT-Infrastruktur einer Wasserversorgung in der Innerschweiz, welcher abgewehrt werden konnte. Dabei sei die Software mehrere tausend Male von bösartigen Anfragen penetriert worden. Um welche konkrete Attacke es sich dabei gehandelt hat, können wir aus der Berichterstattung nicht herleiten.

Unbestritten ist die Tatsache, dass zunehmend Angriffe auf Netzwerke in Versorgungs- und Entsorgungssystemen beobachtet werden. Leitsysteme in diesen Bereichen zählen zu den integralen Bestandteilen **kritischer Infrastrukturen**.
Die klassischen Ziele wie auch die Absichten der Angreifer haben sich geändert; es geht primär nicht um den Diebstahl von Daten, sondern um Störungen der Prozesse und unmittelbar darum, Instabilität zu erzeugen. Ein möglicher Ausfall oder ein unerlaubter Zugriff auf solche Systeme kann ernsthafte Folgen haben.

Im Vergleich zu den einfachen, unkoordinierten Attacken in der Vergangenheit, sind Cyberangriffe heutzutage massiv, vielfältig und gut organisiert, um zielgerichtet Schaden anzurichten. Unter anderem wurden spezielle Malware-Varianten für Attacken gegen kritische Infrastrukturen entwickelt.

Jede Netzwerkkomponente, welche am Internet angeschlossen ist, wird früher oder später angegriffen. Die IP-Adressen werden weltweit permanent, auch von Cyberkriminellen, abgefragt. In den meisten Logdateien einer Firewall können diese Anfragen auch nachgewiesen werden.

## Wie ist die Bedrohungslage meiner Anlage?

In den letzten Jahrzehnten wurden die kritischen Infrastrukturen bei weitem nicht so gut geschützt, wie sie es heute sind. Allerdings ist das alleinige Vertrauen auf traditionellen Schutz nicht mehr zeitgemäss.
IT-Sicherheit besteht aus 75% Mensch (organisatorisch) und nur 25% Technologie.
Darum müssen neue Wege gefunden werden, um moderne Hackerangriffe abzuwehren.

Vermehrt stellen sich die Betreiber daher folgende Fragen:
- Welche Anforderungen werden heute sowie in Zukunft an die IT-Sicherheit gestellt?
- Auf welchem IT-Sicherheitsstand ist meine Anlage?
- Kann meine Anlage einen Cyberangriff abwehren?

Durch einen guten IT-Grundschutz bietet die Architektur eines **Rittmeyer-Systems** genügend Widerstand, um eine Attacke zu überstehen. Grundsätzlich sind unsere Steuerungen so konzipiert, dass sie ohne Server oder Netzwerk mit den letzten Einstellungen autonom im Automatikbetrieb weiterlaufen. Der Internetanschluss wird mit einer Firewall geschützt und ein Zugriff von aussen ist nur über eine verschlüsselte VPN Verbindung möglich. Eine DDoS (Distributed Denial of Service = Verweigerung des Dienstes) Attacke behindert maximal den Fernzugriff oder eine allfällige Kommunikation mit Aussenstationen, welche über das Internet angeschlossenen sind.
Die Netzwerke zwischen Leitsystem (IT) und Automatisierungsstationen (OT) sind voneinander getrennt und verwenden unterschiedliche Protokolle.

## Wie kann ich mich dagegen schützen?

Mit gezielten Schutzmassnahmen lässt sich ein guter IT-Grundschutz aufbauen:
- Verhindern
- Überwachen / Erkennen
- Alarmieren
- Wiederherstellen

Wir beraten und unterstützen Sie gerne, um Fragen zu beantworten, potenzielle Schwachstellen und Bedrohungen frühzeitig zu erkennen und daraus gezielte Schutzmassnahmen zur IT-Sicherheit einzuführen. Unsere zertifizierten ISO-27001-Experten stehen Ihnen mit Kenntnissen sowohl in der operativen Technologie (OT) als auch zur industriellen Cyber-Sicherheit zur Seite. Dabei unterstützen wir Sie / Ihre Organisation von der Ist-Analyse über das Erstellen und Umsetzen eines individuellen IT-Sicherheitskonzepts bis hin zu nachhaltigen Service-Modulen. Security-Vorfälle werden dadurch verringert sowie der Reifegrad der industriellen Cyber-Sicherheit erhöht.

**Branchen-Empfehlung**
Der IKT Minimalstandard (Informations- und Kommunikationstechnologie) ist ein Gemeinschaftswerk des Bundesamtes für wirtschaftliche Landesversorgung (BWL) und dem SVGW und wird voraussichtlich im Frühling 2019 in Kraft treten. Der Verband der Schweizer Elektrizitäts-unternehmen (VSE) verwendet diese Richtlinie bereits und voraussichtlich werden auch die Gasversorgung und die Abwasserbranche das neue Regelwerk für ihre Richtlinien anwenden. Betreibern von kritischen Infrastrukturen wird empfohlen, den IKT-Minimalstandard umzusetzen. Wir helfen Ihnen die Fragen zu beantworten und die richtigen Massnahmen zu bestimmen.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity