

# Risiken und Nebenwirkungen vermeiden: maßgeschneiderte Sicherheitskonzepte

Digitalisierung &amp; IT

Von Michael Wolf

**Step by Step werden Prozesse und Systeme in Unternehmen immer digitaler. Das Internet bzw. die virtuelle Welt verspricht neue betriebswirtschaftliche und volkswirtschaftliche Potenziale. Verschiedene Studien zeigen – bei aller Aufbruchstimmung – dass oft die mittelständischen Unternehmen noch immer bei den Themen Digitalisierung und Industrie 4.0 zögerlich agieren. Das liegt auch an Sicherheitsbedenken – zu Recht.**

## **Der Computer-Virus WannaCry als mahnendes Beispiel**

Genau diese Bedenken haben kürzlich erst neue Nahrung erhalten. Der Computer Virus WannaCry kreierte den bislang umfangreichsten Cyberangriff aller Zeiten. Er infizierte rund 350.000 Systeme in 150 Ländern. Und bewies eins dabei: Vor allem in Deutschland ist die IT-Sicherheit bei weitem noch auf keinem hohen Niveau etabliert. Neben Großkonzernen, Krankenhäusern oder anderer Institutionen und Organisationen wurden in Deutschland vielfach gerade mittelständische Unternehmen Opfer der Cyber-Attacke. Dabei fällt auf, dass die Firmen, die sich dem Cyberangriff erfolgreich widersetzen konnten, über dementsprechend maßgeschneiderte Sicherheitskonzepte und auch größtenteils über Notfallsicherheitskonzepte verfügen.

## **Sicherheitsstrukturen müssen ganzheitlich konzeptioniert werden**

Hier besteht zweifelsohne Handlungsbedarf. Entsprechende Sicherheitskonzepte sollten sich dabei allerdings nicht ausschließlich mit der Sicherung der unternehmensspezifischen IT-Infrastrukturen befassen. Denn mit der Vernetzung und auch Digitalisierung von Verwaltung und Produktion sowie mit Abnehmern, Lieferanten und sonstigen Geschäftspartnern steigen gleichzeitig auch die Risiken für die Informationssicherheit. Um diesen Gefahren zu begegnen, müssen Sicherheitsstrukturen ganzheitlich, also abteilungsübergreifend, gestaltet werden. Der Geschäftsleitung kommt dabei eine tragende Rolle zu. Informationssicherheit ist Chefsache! In der Praxis kann sich die Einführung ganzheitlicher Sicherheitskonzepte als ein äußerst schwieriges Unterfangen darstellen. Dies hat mehrere Gründe: Zum einen fehlt es in den Unternehmen bzw. bei den Mitarbeitern an diesbezüglichem Wissen; zum anderen gibt es über lange Zeiträume gewachsene Strukturen und Prozesse, die sich den erforderlichen Veränderungen oftmals widersetzen.



Michael  
Wolf

Kooperationspartner  
Johannes Müller  
Wirtschaftsberatung (BDU)

*IT-Spezialist  
IT-Architekt  
Penetrationstests*

**„Industrie 4.0 bedeutet eine noch stärkere Vernetzung der klassischen IT mit der Produktion.“**

**Bei allen Chancen, kann ein gezielter Hacker-Angriff dann drastischere Folgen als zuvor haben.**

**Daher sollten sich Unternehmen besonders intensiv und sorgfältig mit dem Thema Sicherheit auseinandersetzen.“**

## Auf zu neuen Ufern: Maßgeschneiderte Sicherheits- und Notfallkonzepte installieren

Wer sich nachhaltig schützen möchte vor den Gefahren der digitalen respektive virtuellen Welt, muss nun konsequent die entsprechenden organisatorischen Maßnahmen angehen. Es werden hier gänzlich neue Sicherheitskonzepte benötigt, die einen ganzheitlichen Ansatz verfolgen. Denn in den mittelständischen Unternehmen wachsen Abteilungen, etwa die Verwaltung und die Produktion, im Rahmen von Industrie 4.0 und der Digitalisierung immer mehr zusammen. Dies erfordert eine neue Ausrichtung der Sicherheitsstrukturen inklusive erprobter Notfallkonzepte.



**„Klassische Anti-Virus- und Firewall-Technologien, wie sie insbesondere aus der Office-IT bekannt ist, bieten im Rahmen von Industrie 4.0 keinen ausreichenden Schutz!“**

**Ganzheitliche Konzepte, die technische Maßnahmen mit organisatorischen Maßnahmen vereint, sind gefragt.**

**Der Cyberangriff durch den Computer-Virus WannaCry sollte jedem Unternehmen klar vor Augen geführt haben, was alles passieren kann.“**

### Maßgeschneiderte Individuallösungen im Fokus

Dafür werden verlässliche Partner benötigt. Wir stellen Ihnen diesbezüglich gerne unser Know-how und unsere Expertise zur Verfügung. Seit Jahrzehnten unterstützen wir erfolgreich Unternehmen bei der Planung, Umsetzung und Kontrolle von spezifischen Sicherheits- und Notfallkonzepten. In unserem weit verstrickten Netzwerk lassen sich zudem zahlreiche Spezialisten für verschiedene Sicherheitslösungen finden, mit denen wir intensiv zusammenarbeiten. So generieren wir grundsätzlich Maßnahmenempfehlungen, die konsequent die neuen Entwicklungen der Digitalisierung bzw. Industrie 4.0 schwerpunktmäßig berücksichtigt.

### Die Gefahr ist allgegenwärtig: Es drohen schwere finanzielle Einbußen

Bei der Sicherheit sollten Sie keine Kompromisse eingehen. Denn - und das hat der Computer-Virus WannaCry nachhaltig gezeigt - die Gefahren bzw. die Herausforderungen, die Industrie 4.0 und das Zusammenwachsen der IT-Systeme und -Infrastrukturen hervorbringen, sind allgegenwärtig. Cyberattacken können zum Beispiel unter Umständen die Produktion stilllegen und damit einen erheblichen finanziellen Schaden anrichten. Oder aber es kommt etwa durch Viren zu einer Manipulation an Fertigungsmaschinen oder maßgeblichen Unternehmensrechnern. Die kann zu minderwertigen Produkten respektive Leistungen führen, an deren Ende auch wieder ein finanzieller Verlust steht. Gerade jetzt, wenn sowohl Produktion als auch Verwaltung an die zentrale IT-Infrastruktur angebunden sind, können Angreifer aus dem Internet mit einer Attacke beispielsweise auf die nunmehr allesamt vernetzten Steuerungssysteme von Anlagen und Maschinen die gesamte Produktion zum Stocken bringen.