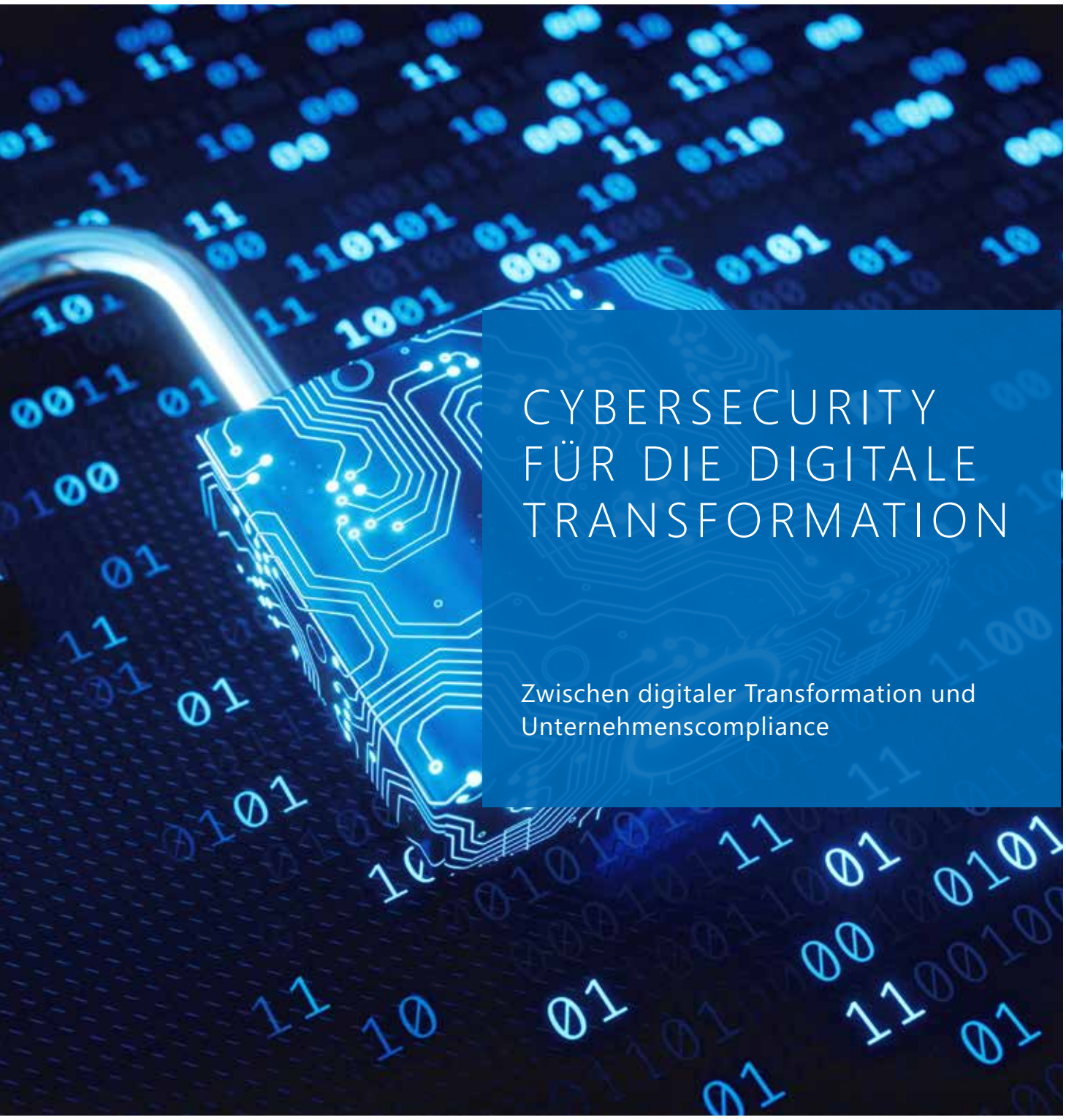


CYBERSECURITY FÜR DIE DIGITALE TRANSFORMATION

Zwischen digitaler Transformation und Unternehmenscompliance

FICHTNER
IT CONSULTING

Managing Cybersecurity:
Informationen schützen. Digitalisierung gestalten.

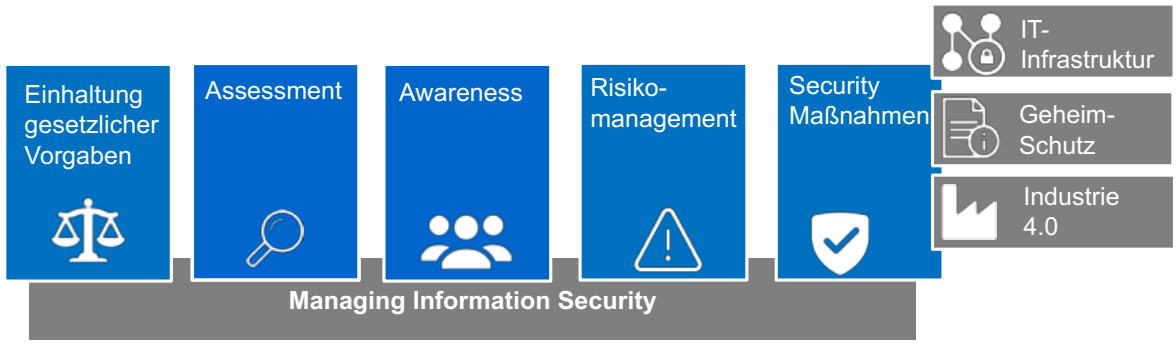
Cyberangriffe und abfließende Informationen sind deutschlandweit für eine Schadensumme von 50Mrd Euro verantwortlich. Dabei sind besonders der innovative Mittelstand sowie Unternehmen und Zulieferer aus dem Bereich Kritischer Infrastrukturen betroffen.

Wie lange kann Ihr Unternehmen noch ohne funktionsfähige IT-Infrastruktur arbeiten?

Diese Frage ist für viele schnell beantwortet, skizziert aber dennoch die Herausforderungen einer vernetzten Geschäftswelt: Die fortschreitende Digitalisierung verändert Geschäftsprozesse und bietet durch einen schnellen Informationsaustausch neue Geschäftsmodelle und Chancen. Gleichzeitig steigt der Professionalisierungsgrad von Angriffen auf IT-Infrastrukturen rapide an. Jedes zweite Unternehmen wurde bereits Opfer eines solches Angriffs. Cyberangriffe sind eine reelle Herausforderung, denen Unternehmen insbesondere im Rahmen der Digitalisierung entgegentreten müssen.

Cyberangriffe sind ein kritisches Unternehmensrisiko

Ein Gros der deutschen Unternehmen betrachtet fehlerhafte oder durch Angriffe kompromittierte IT-Systeme sowie das Abfließen sensibler Unternehmensdaten als Bestandteil der kritischen Unternehmensrisiken. Eine angemessene Steuerung dieser Risiken ist daher genauso notwendig, wie die Betrachtung klassischer betriebswirtschaftlicher Risiken. Voraussetzung ist dabei die Implementierung eines ganzheitlichen Steuerungsrahmens für die Themen Cybersecurity und Informationsschutz.



Wettbewerbsfaktor Cybersecurity und Privacy für die digitale Transformation

Cybersecurity und Informationsschutz sind Managementaufgabe

Eine effiziente Umsetzung setzt eine umfassende Betrachtung der Thematik voraus: Cybersecurity muss von oben gedacht werden, um ein nachhaltiges Sicherheitsbewusstsein innerhalb der Organisation zu schaffen. Gleichzeitig steigt die Anzahl und Komplexität gesetzlicher Anforderungen. Der Nachweis zur Einhaltung dieser Gesetze liegt im Verantwortungsbereich des Managements. Zusätzlich sind viele Unternehmen verpflichtet rechtsverbindliche Cybersecurity-Anforderungen an Dienstleister und Zulieferer weiterzugeben, sodass dieses Thema in der Regel auch innerhalb der Unternehmens Compliance Beachtung finden muss.

Cybersecurity für Industrie 4.0

Die Verschmelzung von klassischer Office IT und Industriesteuersystemen nimmt sukzessive zu. Ebenso steigt die Anzahl gezielter Angriffe auf industrielle Steuersysteme. Unternehmen die industrielle Steuersysteme einsetzen, sind daher zwei wesentlichen Risiken ausgesetzt: Zum einen kann ein Angriff die eigenen Steuersysteme lahmlegen und empfindliche Umsatzeinbußen nach sich ziehen und zum anderen haben manipulative Angriffe nicht selten zur Folge, dass Sicherheitsfunktionen verändert oder gar deaktiviert werden. Damit besteht ein Risiko für Leib und Leben der Personen im Umgang mit den betroffenen Anlagen.

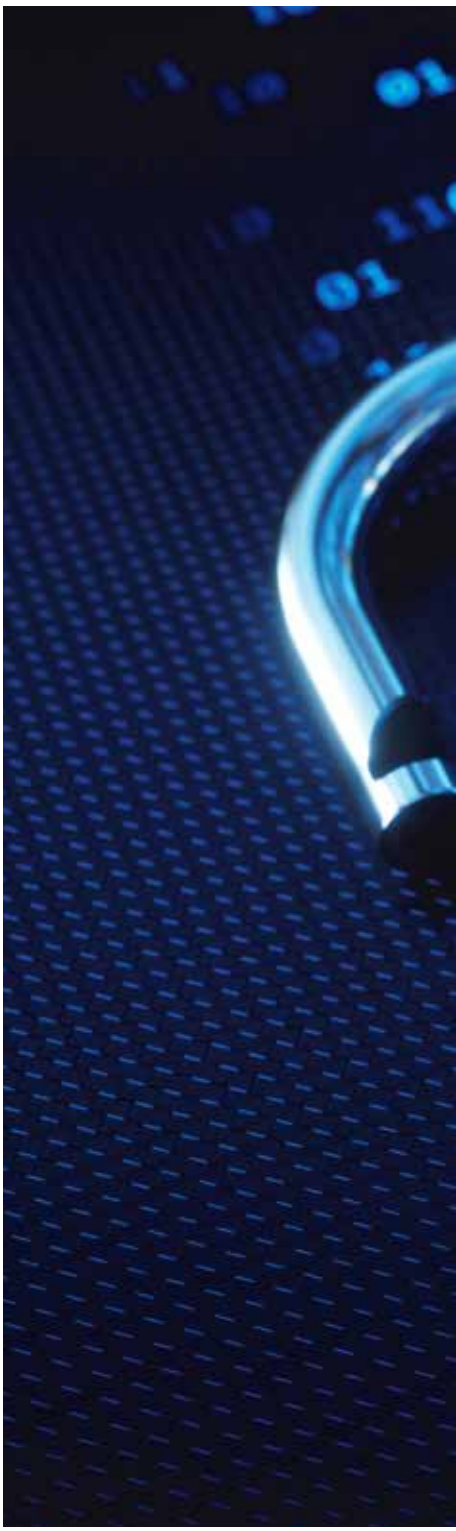
Im Rahmen der Störfallverordnung ist der Betreiber dieser Anlangen in der Pflicht eine Minimierung dieser Cyberrisiken anzustreben.

Wie sollte das Thema Cybersecurity im Unternehmen angegangen werden?

Erfahrungsgemäß stellt insbesondere die Identifizierung kritischer Handlungsfelder und die Entwicklung einer individuellen Cybersecurity Strategie für viele Unternehmen eine große Herausforderung dar.

Dabei gilt es, das Thema ganzheitlich zu betrachten: Ausgehend über gesetzliche Rahmenbedingungen, Kundenanforderungen die sich auf Grund von branchenspezifischen Regularien ergeben bis hin zu operativen Schutzmaßnahmen. Dies zeigt deutlich: eine Cybersecurity-Strategie ist stets individuell und muss zu Ihrem Profil passen. Sicher ist jedoch: Cybersecurity und Informationsschutz sind Basis für eine erfolgreiche digitale Transformation.

Fichtner IT-Consulting hat bereits zahlreiche Unternehmen bei der Anpassung ihrer Cybersecurity Strategie unterstützt. Viele dieser Unternehmen stammen aus dem besonders sensiblen Sektor der kritischen Infrastrukturen. Im Zuge unser Projekte steht für uns die individuelle Anpassung und Implementierung eines maßgeschneiderten Managementrahmens der Informationssicherheit stets im Zentrum des Handelns: Auf diese Weise setzen wir nicht nur ein konsistentes Sicherheitskonzept um, sondern schaffen zugleich einen spürbareren Mehrwert für betroffene Unternehmen und stellen damit gleichzeitig und die Weichen für den digitalen Wandel. Denn auch Digitalisierung funktioniert nicht ohne Informationssicherheit.



FICHTNER
IT CONSULTING

Fichtner IT Consulting ist das IT-Kompetenzzentrum der seit 1922 inhabergeführten Fichtner-Gruppe mit rund 1.500 Mitarbeitern in über 60 Ländern. Wir konzipieren und realisieren Informationslogistik für technische Netze, Anlagen und Infrastruktur. Unsere Branchenkenntnis und das Prozess-Know-how verbinden wir mit aktuellster Technologiekompetenz und liefern so innovative und wirtschaftliche Lösungen für Ihren Erfolg. Die Gewinnung, Strukturierung, Verknüpfung sowie Aufbereitung und Präsentation von Informationen – auch im räumlichen Bezug – sind dabei der Schlüssel für effiziente und effektive Lösungen.

Fichtner IT Consulting GmbH
Sarweystraße 3
70191 Stuttgart
Deutschland

Telefon: +49 (0)711 8995-10
Telefax: +49 (0)711 8995-1450
info@fit.fichtner.de
www.fit.fichtner.de