



Branchencheck Cyber Security

Cyber Risiken im Maschinenbau

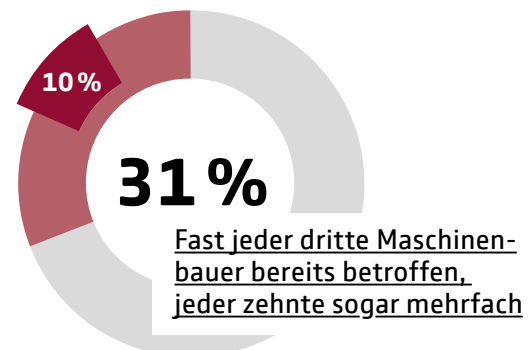
Das Risiko von Cyberattacken auf die stark digitalisierte und vernetzte Branche ist hoch, doch die Gefahr wird von vielen mittelständischen Maschinenbauern unterschätzt. Die IT-Sicherheit der Branche zeigt Lücken – und diese werden von Kriminellen konsequent genutzt, wie Analysen im Auftrag der deutschen Versicherer zeigen.

Gefahr erkannt?

In einer Forsa-Umfrage gab jedes dritte Unternehmen an, bereits Opfer erfolgreicher Cyberattacken gewesen zu sein, jedes zehnte Unternehmen war sogar mehrfach betroffen. Infolge der Attacken standen die meisten Betriebe zeitweise still und mussten Zeit und Geld in die Wiederherstellung ihrer Systeme investieren; teilweise zahlten die Maschinenbauer für ihre gesperrten Daten und IT-Systeme auch Lösegelder.

Dennoch nehmen viele Maschinenbauer die Bedrohungen durch Cyberkriminelle kaum ernst. Vier von zehn Maschinenbauern schätzen das Cyberisiko der Branche als gering ein, für das eigene Unternehmen können sogar 55 Prozent nur ein geringes Risiko erkennen.

Maschinenbauer sind beliebte Ziele von Cyberkriminellen



Einschätzung des eigenen Risikos wirft Fragen auf



Für die Initiative Cybersicher hat Forsa die für Internetsicherheit zuständigen Mitarbeiter von 100 kleinen und mittleren Maschinenbauern befragt. Die PPI AG hat mit ihrem Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 500 mittelständischen Maschinenbauern passiv getestet und dabei alle öffentlich einsehbaren Informationen aus Sicht eines potentiellen Angreifers erfasst und bewertet. Die Forsa-Interviews fanden im Februar, die Tests im März und April 2020 statt.

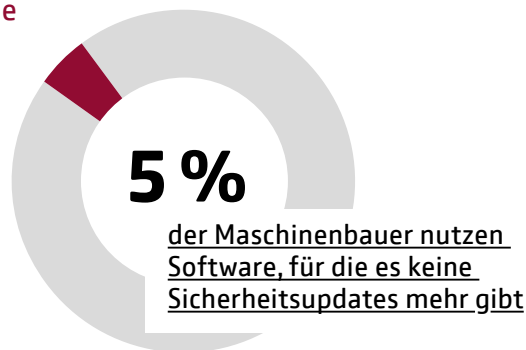
Angriffe auf anfällige Systeme

Als Ergebnis der unzureichenden Risikowahrnehmung zeigen sich weit verbreitete Mängel bei der IT-Sicherheit. Eine Untersuchung der IT-Systeme 500 mittelständischer Maschinenbauer mit Hilfe des Analyse-Tools Cysmo ergab unter anderem, dass fünf Prozent der Unternehmen veraltete Software einsetzen, für die es keine Sicherheitsupdates mehr gibt. Auch der Blick ins Darknet war ergiebig: Hier fanden sich Daten von fast der Hälfte (45%) der Unternehmen, darunter fast 8.000 E-Mail-/Passwort-Kombinationen von Mitarbeitern.

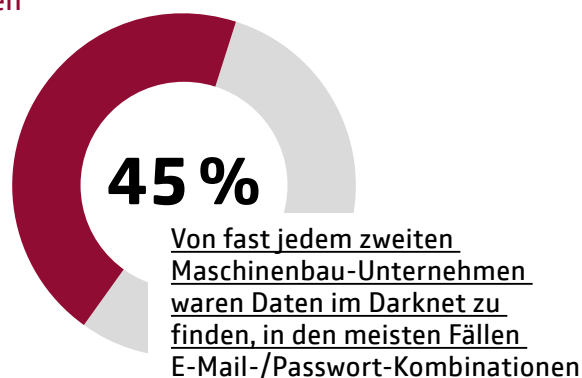
Akuten Handlungsbedarf zeigen auch die Selbstauskünfte der befragten Maschinenbauer: Fast die Hälfte der Unternehmen (42%) sind auf einen IT-Notfall nicht vorbereitet, aber 47 Prozent erlauben es Mitarbeitern, ihre privaten Geräte in der IT-Umgebung des Unternehmens zu nutzen. Zudem erfüllt nur ein Drittel die wichtigsten Basis-Anforderungen an die IT-Sicherheit; unter anderem werden Sicherungskopien nicht überall sicher aufbewahrt und getestet.

Vielen Unternehmen fehlt schon die Basis für umfassende IT-Sicherheit. Ergebnis für die 10 Grundanforderungen des GDV-Cyber-Sicherheitschecks.

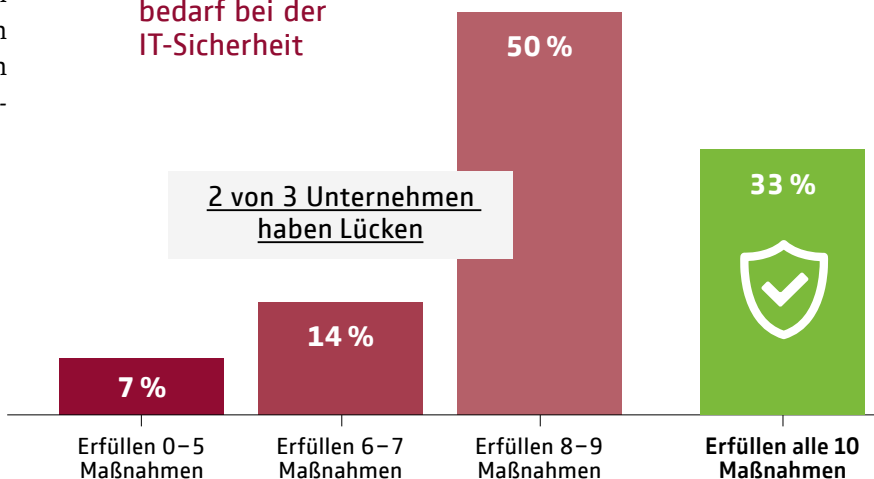
Veraltete Systeme sind tickende Zeitbomben



Sensible Daten im Darknet



Akuter Handlungsbedarf bei der IT-Sicherheit



Machen Sie den Check!

Der kostenlose **Cyber-Sicherheitscheck des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können.