CYBER SICHER

Eine Initiative der deutschen Versicherer.

Branchencheck Cyber Security

Cyberrisiken in der Elektroindustrie

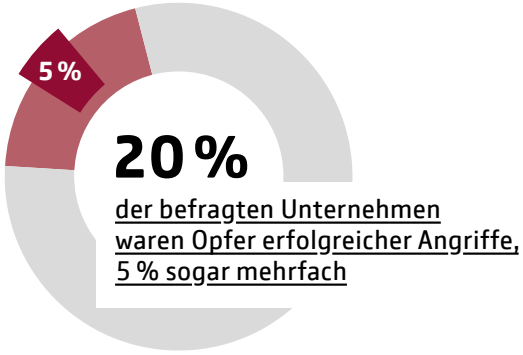
Das Risiko von Cyberattacken auf die stark digitalisierte und vernetzte Branche ist hoch, doch die Gefahr wird von vielen mittelständischen Unternehmen der Elektroindustrie unterschätzt. Die IT-Sicherheit der Branche zeigt Lücken – und diese werden von Kriminellen konsequent genutzt, wie Analysen im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

Gefahr erkannt?

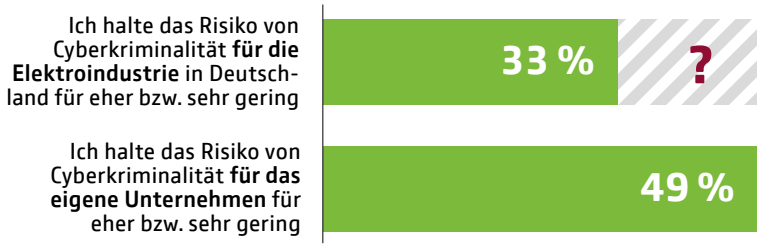
In einer Forsa-Umfrage gab jedes fünfte Unternehmen an, bereits Opfer erfolgreicher Cyberattacken gewesen zu sein, fünf Prozent waren sogar schon mehrfach betroffen. Infolge der Attacken standen die meisten Betriebe zeitweise still und mussten Zeit und Geld in die Wiederherstellung ihrer Systeme investieren;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

Dennoch nehmen in der Elektro industrie viele die Bedrohungen durch Cyberkriminelle kaum ernst: Die Hälfte der Befragten schätzt das Cyberrisiko für das eigene Unternehmen als gering ein; 40 Prozent der Unternehmen wollen in den kommenden zwei Jahren auch nicht weiter in IT-Sicherheit investieren.

Die Elektroindustrie ist ein beliebtes Ziel 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 Unternehmen der Elektroindustrie befragt. Die PPI AG hat mit ihem Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 500 mittelständischen Unternehmen der Elektroindustrie 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.

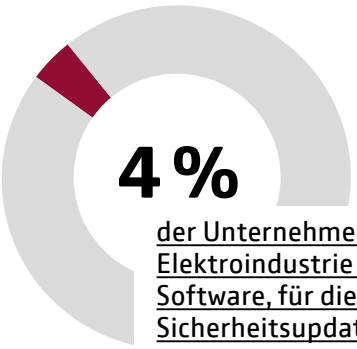
Angriffe auf anfällige Systeme

Als Ergebnis der unzureichenden Risikowahrnehmung und geringen Investitionsbereitschaft zeigen sich weit verbreitete Mängel bei der IT-Sicherheit. Eine Untersuchung der IT-Systeme 500 mittelständischer Unternehmen der Elektroindustrie mit Hilfe des Analyse-Tools Cysmo ergab unter anderem, dass vier Prozent der Unternehmen veraltete Software einsetzen, für die es keine Sicherheitsupdates mehr gibt. Sehr ergiebig war auch der Blick ins Darknet: Hier fanden sich Daten von mehr als der Hälfte (53 %) der Unternehmen, darunter rund 10.500 E-Mail-/Passwort-Kombinationen von Mitarbeitern.

Akuten Handlungsbedarf zeigen auch die Selbstauskünfte der Branche: Fast die Hälfte der Unternehmen (43 %) sind auf einen IT-Notfall nicht vorbereitet, aber 49 Prozent erlauben es Mitarbeitern, ihre privaten Geräte in der IT-Umgebung des Unternehmens zu nutzen. Die wichtigsten Basis-Anforderungen an die IT-Sicherheit erfüllen zudem nur 29 Prozent der Befragten; unter anderem werden auch sehr einfache Passwörter zugelassen oder Sicherungskopien nicht sicher aufbewahrt und getestet.

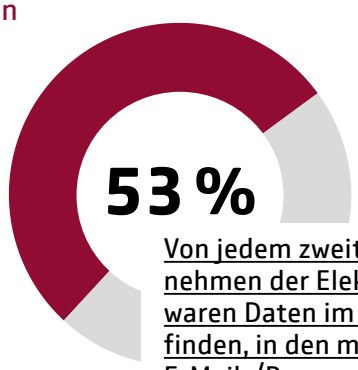
Vielen Unternehmen fehlt schon die Basis für umfassende IT-Sicherheit. Ergebnis für die 10 Grundanforderungen des GDV-Cyber-Sicherheitschecks.

Veraltete Systeme sind tickende Zeitbomben



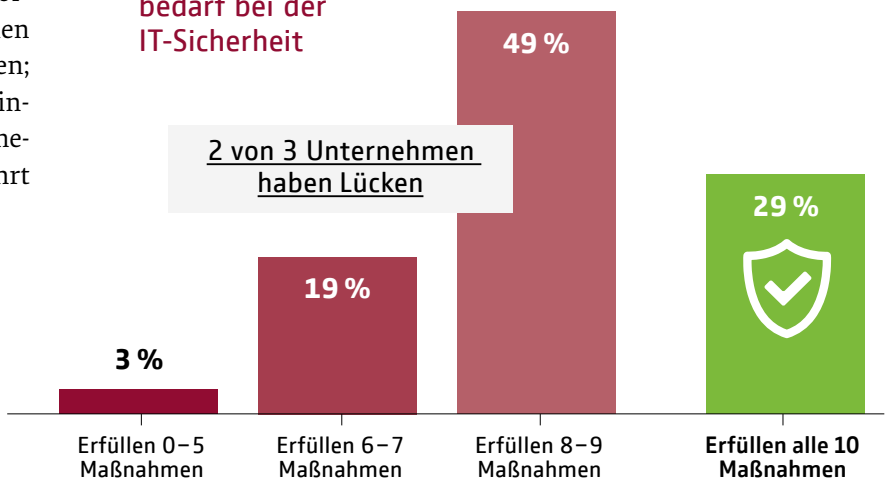
der Unternehmen in der Elektroindustrie nutzen Software, für die es keine Sicherheitsupdates mehr gibt

Sensible Daten im Darknet



Von jedem zweiten Unternehmen der Elektroindustrie waren Daten im Darknet zu finden, in den meisten Fällen E-Mail-/Passwort-Kombinationen

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.