Branchencheck Cyber Security

Cyberrisiken in der chemischen Industrie

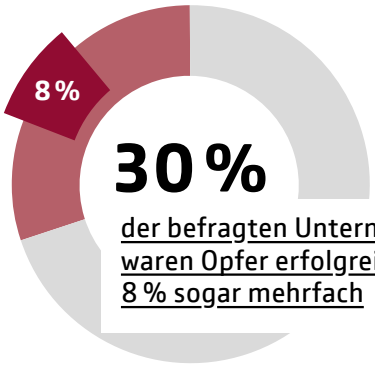
Das Risiko von Cyberattacken auf die Branche ist hoch, doch viele mittelständische Chemiehersteller sind auf die Angriffe schlecht vorbereitet. Die IT-Sicherheit der Branche zeigt Lücken – die von Kriminellen auch ausgenutzt werden, wie Analysen im Auftrag der deutschen Versicherer zeigen.

Gefahr erkannt?

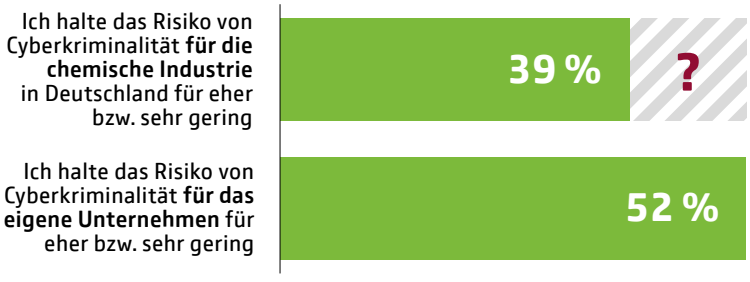
In einer Forsa-Umfrage gab fast jedes dritte Unternehmen (30%) an, bereits Opfer erfolgreicher Cyberattacken gewesen zu sein, acht Prozent waren sogar schon mehrfach betroffen. Nach einer erfolgreichen Attacke stand fast die Hälfte der Betriebe zeitweise still. Weitere finanzielle Schäden entstanden durch den hohen Aufwand, mit dem Angriffe analysiert und entwendete oder gesperrte Daten wiederhergestellt werden mussten.

Trotz dieser hohen Betroffenheit nehmen viele mittelständische Chemiehersteller die Bedrohungen durch Cyberkriminelle nicht ernst genug: 52 Prozent der Befragten schätzen das Cyberrisiko für das eigene Unternehmen als gering ein; die Hälfte der Unternehmen will in den kommenden zwei Jahren auch nicht weiter in IT-Sicherheit investieren.

Die chemische Industrie ist ein beliebtes Ziel von Cyberkriminellen



Einschätzung des eigenen Risikos wirft Fragen auf



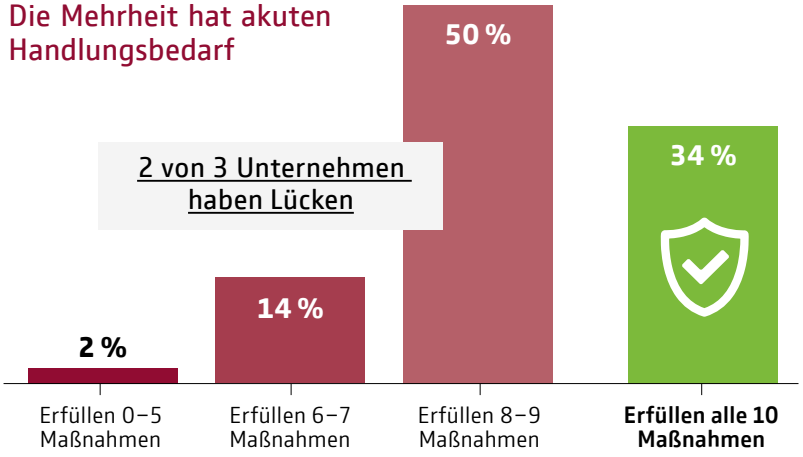
Für die Initiative Cybersicher hat Forsa die für Internetsicherheit zuständigen Mitarbeiter von 100 kleinen und mittleren Chemieherstellern befragt. Die PPI AG hat mit ihrem Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 510 mittelständischen Unternehmen der chemischen Industrie passiv getestet 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

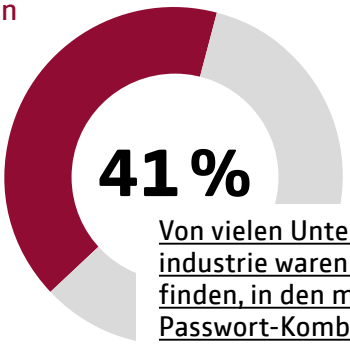
Als Ergebnis der unzureichenden Risikowahrnehmung und geringen Investitionsbereitschaft zeigen sich weit verbreitete Mängel bei der IT-Sicherheit. Zwar werden fast überall sichere Passwörter erzwungen und Sicherheitsupdates automatisch eingespielt, aber 39 Prozent verzichten darauf, die Sicherungskopien ihrer Daten auch zu testen. Insgesamt erfüllt nur ein Drittel der befragten Unternehmen (34%) die zehn wichtigsten Basis-Anforderungen an die IT-Sicherheit. Auch der Blick ins Darknet war ergiebig: Bei einer Analyse von 510 Mittelständlern der Chemieindustrie mit Hilfe des Analyse-Tools Cysmo konnten von 208 Unternehmen (41%) Daten im Darknet gefunden werden, darunter mehr als 10.000 E-Mail-/Passwort-Kombinationen von Mitarbeitern.

Akuter Handlungsbedarf ergibt sich auch aus weiteren Ergebnissen der Umfrage: In jedem dritten Unternehmen (33%) ist niemand explizit für die Informationssicherheit verantwortlich, ebenfalls ein Drittel (35%) hat für einen Cyberangriff weder ein Notfallkonzept noch eine Vereinbarung mit ihrem IT-Dienstleister. Das kann im Ernstfall gravierende Konsequenzen haben, denn die Abhängigkeit von einer funktionierenden IT ist in der chemischen Industrie hoch: Zwei von drei befragten Unternehmen (66%) könnten bei einem Ausfall ihrer IT-Systeme kaum noch arbeiten.

Die Mehrheit hat akuten Handlungsbedarf



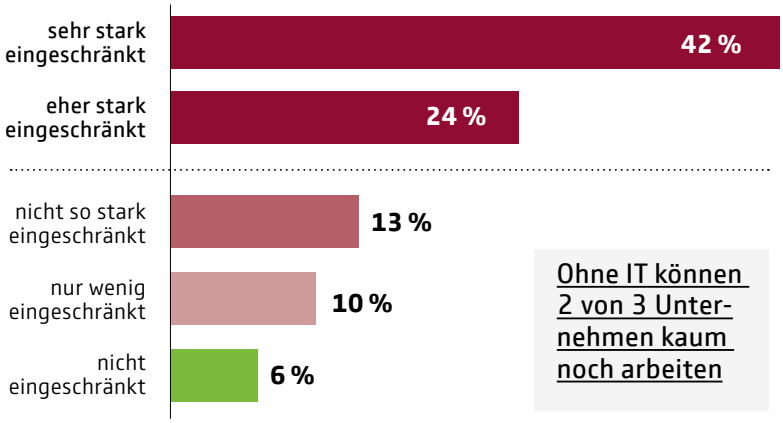
Sensible Daten im Darknet



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

Eine nicht funktionierende IT legt in der chemischen Industrie die meisten Unternehmen lahm

Würde die IT mehrere Tage ausfallen, wäre Ihr Betrieb …



Ohne IT können 2 von 3 Unternehmen kaum noch arbeiten

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.