



Cybersicherheit im Handwerk: Wie gut sind Betriebe auf Cybervorfälle vorbereitet?

*Laut Sophos-Umfrage unter 200 Handwerksbetrieben fühlt sich die Mehrheit gut vorbereitet
– rund ein Drittel sieht Defizite*

Cybersicherheit ist für viele Handwerksbetriebe heute Teil der täglichen Arbeit. Digitale Systeme, vernetzte Anwendungen und mobile Arbeitsweisen prägen Abläufe in Werkstätten, auf Baustellen und in der Verwaltung. Sophos ist im Rahmen einer Umfrage unter Handwerks- und handwerksnahen Betrieben der Frage nachgegangen, wie die Cybersicherheit organisiert ist und wie Betriebe ihre eigene Vorbereitung einschätzen.

Cybersicherheit ist organisatorisch verankert und häufig von extern unterstützt

In den meisten befragten Handwerks- und handwerksnahen Betrieben ist Cybersicherheit klar zugeordnet. 67 Prozent der Unternehmen betreiben Cybersicherheit inhouse und mit zusätzlicher Unterstützung von externen Dienstleistern. Weitere 19,5 Prozent setzen ausschließlich auf interne Ressourcen, während 12,5 Prozent das Thema vollständig an externe Anbieter ausgelagert haben. Lediglich 1 Prozent der Betriebe gibt an, dass es keine klare Zuständigkeit gibt.

Über die befragten Handwerksbereiche und Betriebsgrößen hinweg zeigen sich dabei weitgehend vergleichbare organisatorische Strukturen. Eine Ausnahme bildet das Bekleidungs-, Textil- und Lederhandwerk: Hier lagern 42,9 Prozent der Unternehmen Cybersicherheit vollständig an externe Dienstleister aus.

Absicherung digital unterstützter Prozesse

Digitale Vernetzung ist in vielen Handwerksbetrieben fester Bestandteil der täglichen Arbeit – etwa durch Maschinensteuerungen, digital angebundene Werkzeuge oder mobile Endgeräte auf Baustellen. Entsprechend stellt sich für viele Betriebe die Frage, wie diese digital unterstützten Prozesse und Systeme abgesichert werden.

58 Prozent der befragten Unternehmen geben an, für vernetzte Systeme klare Sicherheitsvorgaben, regelmäßige Updates und Zugriffskontrollen etabliert zu haben. 29 Prozent sichern einzelne Geräte oder Anwendungen ab, jedoch nicht durchgängig. 10,5 Prozent verlassen sich bei der Absicherung vernetzter Systeme auf die Sicherheitskonzepte der Hersteller oder Anbieter.

Die eigene Vorbereitung wird unterschiedlich eingeschätzt

Bei der Einschätzung der eigenen Vorbereitung auf einen Cyberangriff ergibt sich ein differenziertes Bild. 20 Prozent der befragten Unternehmen schätzen ihre Vorbereitung als sehr gut ein und gehen davon aus, den Betrieb sofort wieder aufnehmen zu können. Weitere 44 Prozent geben an, gut vorbereitet zu sein und nach kurzer Zeit wieder arbeitsfähig zu sein.

Demgegenüber geben 30,5 Prozent an, im Falle eines Cyberangriffs nur eingeschränkt arbeitsfähig zu sein. Weitere 5,5 Prozent fühlen sich schlecht vorbereitet und rechnen mit längeren Ausfallzeiten. Einzelne Unternehmen bestätigen, gar nicht vorbereitet zu sein oder können ihre Situation nicht sicher einschätzen.

Auffällig ist erneut das Bekleidungs-, Textil- und Lederhandwerk: 28,6 Prozent der befragten Betriebe attestieren sich eine schlechte Vorbereitung für den Fall eines Cyberangriffs.

Fazit: Klare Strukturen, aber unterschiedliche Bereitschaft

Die Vorbereitung auf Cybervorfälle variiert im Handwerksumfeld stark. Während sich 64 Prozent der Betriebe gut oder sehr gut gerüstet fühlen, sehen 36 Prozent noch Nachholbedarf.

„Cybersicherheit ist im Handwerk heute fest in den betrieblichen Abläufen verankert – häufig in klar definierten organisatorischen Strukturen. Transparenz über Abläufe, Zuständigkeiten und den eigenen Vorbereitungsstand spielt dabei eine zentrale Rolle. Allerdings liegt die Einschätzung im Handwerk bezüglich der Cyberresilienz deutlich unter dem Niveau von größeren Unternehmen“, sagt Michael Veit, Sicherheitsexperte bei Sophos. „Für die Angreifer macht es jedoch kaum einen Unterschied, wer attackiert wird. Auch kleinere Unternehmen haben wertvolle Daten und Informationen, die Cyberkriminelle für ihre Zwecke missbrauchen. Daher ist es wichtig, dass wirkungsvolle Cybersicherheit, wenn nötig mit externer Expertise, auf einem sehr hohen Niveau stattfindet.“

Vier Handlungsempfehlungen für Handwerksbetriebe

1. **Klare Zuständigkeiten festlegen:** Auch bei der Zusammenarbeit mit externen Dienstleistern sollten Verantwortlichkeiten und Abläufe eindeutig geregelt sein.
2. **Digitale Systeme systematisch berücksichtigen:** IT-Systeme, Anwendungen und vernetzte Prozesse sollten regelmäßig überprüft und in Sicherheitsmaßnahmen einbezogen werden.
3. **Resilienz und Vorbereitung regelmäßig überprüfen:** Eine regelmäßige Überprüfung der eigenen Wiederanlauffähigkeit nach Cybervorfällen unterstützt die Einschätzung der tatsächlichen Situation.
4. **Cybersicherheit kontinuierlich weiterentwickeln:** Technische und organisatorische Schutzmaßnahmen sollten fortlaufend überprüft und angepasst werden.

Über die Umfrage

Grundlage der Auswertung ist eine quantitative Befragung von 200 Unternehmen, die im Dezember 2025 und Januar 2026 von Techconsult im Auftrag von Sophos durchgeführt wurde.

Befragt wurden Betriebe folgender Bereiche: Bau- und Ausbaugewerbe, Elektro- und Metallhandwerk, Holz- und Kunststoffverarbeitung, Lebensmittelhandwerk, Bekleidungs-, Textil- und Lederhandwerk, Gesundheits-, Körperpflege- und Reinigungsgewerbe, Kunsthandwerk sowie Industrie mit handwerklichem Bezug, technische Dienstleistungen und weitere handwerksnahe Betriebe.

Die Befragung berücksichtigte Unternehmen mit mehr als 20, 50, 100 sowie 250 Mitarbeitenden.

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de