# PRESSEMITTEILUNG

Nr. 12 01.10.2025

**CYBERsicher Lagebild 2025: Die aktuelle Cyberbedrohungslage für kleine und mittlere Unternehmen**

**Der Report der Transferstelle Cybersicherheit im Mittelstand wirft einen Blick auf die aktuelle Bedrohungslage für kleine und mittlere Unternehmen**

Berlin – Passend zum Start des Cybersicherheitsmonats 2025 veröffentlicht die Transferstelle Cybersicherheit im Mittelstand, ein gefördertes Projekt des Bundesministeriums für Wirtschaft und Energie, das CYBERsicher Lagebild. Neben einer Auswertung von Angriffen auf Unternehmen wirft der Report auch einen detaillierten Blick auf die Entwicklungen im Bereich Ransomware- und Phishing-Attacken. Zusätzlich wird aufgezeigt, welche Schutzmaßnahmen von Unternehmer:innen bereits konsequent umgesetzt werden und in welchen Bereichen nachgebessert werden muss.

**Deutsche Unternehmen im Visier der Cyberkriminellen**

Die Bedrohungslage für Unternehmen in Europa und in Deutschland spitzt sich zu. Die Anzahl an Angriffen durch Hacker steigt kontinuierlich. Besonders besorgniserregend: Hackerattacken auf deutsche Unternehmen, die auf Leakseiten veröffentlicht wurden, haben sich Schätzungen zufolge zwischen den Jahren 2021 bis 2024 mehr als vervierfacht. Damit ist Deutschland trauriger Spitzenreiter, gefolgt von Italien, Frankreich und Spanien.

Auch Zahlen des BKA belegen diese Entwicklung. Laut der polizeilichen Kriminalstatistik 2024 richten sich 80 Prozent der 950 ausgewerteten Ransomware-Angriffe gegen kleine und mittlere Unternehmen. In 251 Fällen konnte zusätzlich über eine Auswertung der Plattform ransomware.live ein Datenabfluss nachgewiesen werden.

„Spätestens jetzt sollten mittelständische Unternehmen die Lage ernst nehmen und entsprechende Maßnahmen zur Absicherung ihrer Betriebe konsequent umsetzen“, ordnet **Dirk Achenbach, Projektleiter der Transferstelle Cybersicherheit im Mittelstand**, die Erkenntnisse ein. Bei einem Blick auf die Angriffsverteilung auf kleine und mittlere Unternehmen je Bundesland zeigt sich, dass die Unternehmen in Berlin und Bremen überdurchschnittlich oft von Cyberangriffen betroffen sind. Unternehmen in Mecklenburg-Vorpommern, Bayern und im Saarland stehen bei Cyberkriminellen weniger im Fokus.

**Eine Cybergefahr mit vielen Gesichtern**

Mit Daten aus dem Selbstcheck der CYBERsicher Notfallhilfe[1] wird aufgezeigt, von welchen Angriffsformen kleine und mittlere Unternehmen besonders betroffen sind und welche Bereiche besonders fokussiert werden sollten. Die Ergebnisse der Auswertung zeigen, dass sich die meisten Nutzer:innen aufgrund von verdächtigen E-Mails an die Plattform wenden. Auch menschliches Fehlverhalten und verdächtiges Systemverhalten führen dazu, dass Nutzer:innen einen IT-Notfall befürchten. Fast jede zehnte Person (9 Prozent) gab im Selbstcheck an, Opfer von Erpressung geworden zu sein.

[1] Der Selbstcheck der CYBERsicher Notfallhilfe wurde bereits von über 1.000 Personen genutzt. Er gibt den Nutzer:innen eine Einschätzung, ob ein Angriff tatsächlich vorliegt.



Der Mittelstand. BVMW e. V. • Bundeszentrale • Leiter Presse und Kommunikation: Lutz Kordges • Potsdamer Straße 7 • 10785 Berlin
Telefon: 030 533206-302 • presse@bvmw.de • www.bvmw.de

**Der Faktor Mensch in der Cybersicherheit**

Neben technischen Schwachstellen sind die Mitarbeitenden von kleinen und mittleren Unternehmen ein beliebtes Angriffsziel. Vor allem mit Phishing-Angriffen sind Cyberkriminelle sehr erfolgreich und fokussieren häufig Personen in Führungspositionen. Das Lagebild zeigt, dass Geschäftsführende durchschnittlich 57 gezielte Phishing-Angriffe pro Jahr abwehren müssen. Bei IT-Verantwortlichen sind es immerhin noch 40 gezielte Phishing-Attacken. Auch der Blick auf die Bundesbürger:innen ist alarmierend. Jede:r sechste Bundesbürger:in hat einen Phishing-Angriff nicht als solchen erkannt. Mehr als jede:r zehnte Betroffene (13 Prozent) hat anschließend nicht die Zugangsdaten geändert.

**Das Phänomen Ransomware**

Nach dem initialen Zugang zu den Unternehmensdaten, in den meisten Fällen durch Phishing-Attacken, folgen in vielen Fällen Ransomware-Angriffe. Die Verschlüsselungstrojaner machen wichtige Daten unlesbar und die Cyberkriminellen fordern ein Lösegeld, um die Daten wieder zu entschlüsseln. Das Lagebild zeigt, dass von fast allen Akteuren Phishing verwendet wird und aktuell in den meisten Fällen mit Double Extortion gerechnet werden muss. Dabei handelt es sich um eine doppelte Erpressung in Bezug auf zunächst die Verschlüsselung und dann die Veröffentlichung der gestohlenen Daten.

**So schützt sich der Mittelstand vor Cyberangriffen**

Anhand der Auswertung der Daten des CYBERsicher Checks, bei dem Nutzer:innen den Stand ihrer IT-Sicherheit anhand des Schulnotensystems bewerten, lässt sich ablesen, welche Sicherheitsmaßnahmen kleine und mittlere Unternehmen in ihren Betrieben umsetzen. Das Lagebild zeigt, dass die meisten Unternehmen ein gutes Konzept für Sicherheitskopien zu besitzen scheinen. Bei Schulungen gibt es ein gemischtes Bild. Unliebsam hingegen scheinen Schutzbedarfsanalysen zu sein.

**KI und Deepfakes: So verändert sich die Cyberlandschaft**

KI-generierte Phishing-Mails sind mittlerweile hochprofessionell, sodass mehr als die Hälfte der Empfänger:innen (60 Prozent) diese nicht als Phishing erkennen. Auch Deepfake-Angriffe, bei denen gefälschte Medieninhalte zum Einsatz kommen, wachsen stark. Allein in Deutschland haben sich im ersten Quartal 2025 Deepfake-Angriffe im Vergleich zum Vorjahr um ganze 1100 Prozent erhöht.

„Der Einsatz von KI wird nicht nur die Anzahl von Cyberangriffen weiter erhöhen, sondern die Attacken auch professionalisieren. Für Betroffene wird es umso schwieriger, betrügerische Nachrichten als Phishing zu erkennen und entsprechend zu reagieren. Umso wichtiger ist es, Mitarbeitende kontinuierlich über neue Betrugsmaschen zu informieren und dadurch zu sensibilisieren“, sagt Marc Dönges, Projektleiter der Transferstelle Cybersicherheit im Mittelstand.

**Schnelle Unterstützung im Ernstfall**

Die CYBERsicher Notfallhilfe unterstützt Nutzer:innen im Ernstfall schnell und unkompliziert. Innerhalb weniger Minuten erhalten sie konkrete Rückmeldungen aus einem großen Netzwerk von Dienstleistern – anonym, unverbindlich


Der Mittelstand. BVMW e. V. • Bundeszentrale • Leiter Presse und Kommunikation: Lutz Kordges • Potsdamer Straße 7 • 10785 Berlin
Telefon: 030 533206-302 • presse@bvmw.de • www.bvmw.de

und mit einer transparenten Übersicht zu Leistungen, Aufwand und Kosten. Die Auswertung der Plattformdaten zeigt, dass das Ausfüllen des Onlineformulars zur Dienstleistersuche im IT-Notfall nur 11 Minuten im Durchschnitt dauert. Zwischen einer Anfrage des Betroffenen und der ersten Rückmeldung durch einen Dienstleister vergehen im Durchschnitt sogar nur acht Minuten. Und die Dienstleister können in der Regel in unter fünf Stunden nach erfolgter Anfrage mit ihrer Unterstützung beginnen.

**Der europäische Monat der Cybersicherheit**

Das CYBERsicher Lagebild wird im Rahmen des europäischen Monats der Cybersicherheit veröffentlicht. Die Transferstelle Cybersicherheit im Mittelstand rückt die digitale Sicherheit von kleinen und mittleren Unternehmen in den Fokus. Unter dem Motto „Vier Wochen – vier Trendthemen“ erhalten Betriebe im Oktober praxisnahe Impulse, wie sie sich wirksam vor Cyberangriffen schützen können - kostenfrei, anbieterneutral und passgenau auf die Realität des Mittelstands zugeschnitten.

Zur Webseite der Transferstelle Cybersicherheit: https://transferstelle-cybersicherheit.de/

Zum CYBERsicher Lagebild: https://transferstelle-cybersicherheit.de/material/das-cybersicher-lagebild/

Zum Cybersicherheitsmonat: https://transferstelle-cybersicherheit.de/cybersicherheitsmonat-2025/

**Über die Transferstelle Cybersicherheit im Mittelstand**

Ziel des Förderprojektes ist es, das Cybersicherheitsniveau von kleinen und mittleren Unternehmen, Handwerksbetrieben und Start-ups für eine sichere digitale Transformation durch Prävention, Detektion und Reaktion zu erhöhen. Über Informations- und Qualifikationsformate, zahlreiche Veranstaltungen bundesweit, eine Detektions- und Reaktionsplattform für Cyberangriffe und ein breites Netzwerk an Partnern wollen wir das Cybersicherheitsniveau im Mittelstand zu erhöhen und Unternehmen resilienter machen. Das Projekt wird von Der Mittelstand, BVMW e.V., dem FZI Forschungszentrum Informatik, der Leibniz Universität Hannover – Institut für Berufspädagogik und Erwachsenenbildung und dem tti Technologietransfer und Innovationsförderung Magdeburg GmbH durchgeführt.

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung mit dem Schwerpunkt Künstliche Intelligenz. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Für weiterführende Informationen kontaktieren Sie bitte:

**Johanna Baldus**
Projektmanagerin Presse- und Öffentlichkeitsarbeit
E-Mail: info@transferstelle-cybersicherheit.de
Der Mittelstand, BVMW e.V.
Bundeszentrale
Potsdamer Straße 7 | Potsdamer Platz
10785 Berlin

# PRESSEMITTEILUNG

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

**Über den Verband**

Der Mittelstand. BVMW e.V. ist die größte, politisch unabhängige und branchenübergreifende Interessenvereinigung des deutschen Mittelstands.

Weitere Informationen unter: **www.bvmw.de**



Der Mittelstand. BVMW e. V. • Bundeszentrale • Leiter Presse und Kommunikation: Lutz Kordges • Potsdamer Straße 7 • 10785 Berlin
Telefon: 030 533206-302 • presse@bvmw.de • www.bvmw.de