



# IT-Sicherheit im Erzgebirge: Warum der Mittelstand jetzt handeln muss

MARCUS SCHÖNFELD



Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

Mittelstand-  
Digital

aufgrund eines Beschlusses  
des Deutschen Bundestages

In diesem „Nachgelesen“ erfahren Sie

- warum IT-Sicherheit im Erzgebirge vom Randthema zur dauerhaften Unternehmensaufgabe geworden ist,
- welche besonderen Herausforderungen IT-Sicherheit für kleine und mittlere Unternehmen in der Region mit sich bringt,
- wie das Mittelstand-Digital Zentrum Chemnitz IT-Sicherheit systematisch einordnet und Unternehmen unterstützt,
- warum Vorsorge wichtiger ist als ein falsches Sicherheitsgefühl,
- weshalb regelmäßige Netzwerkprüfungen und sensibilisierte Mitarbeitende zentrale Schutzfaktoren sind,
- wie Phishing-Angriffe für Unternehmen zur realen Erfahrung werden können,
- warum ein IT-Notfallplan Unternehmen auf den Ernstfall vorbereitet,
- welche Unterstützungsangebote und Impulse regionale Unternehmen nutzen können,
- warum IT-Sicherheit eine Voraussetzung für Zukunftsfähigkeit ist.

## Impressum

### **HERAUSGEBER**

Mittelstand-Digital Zentrum Chemnitz  
c/o TU Chemnitz  
Erfenschlager Str. 73, 09125 Chemnitz  
Tel: 0371 531 19935 Fax: 0371 531 819935  
info@digitalzentrum-chemnitz.de  
www.digitalzentrum-chemnitz.de

**REDAKTION** Anikó Lessi

### **GESTALTUNG UND PRODUKTION**

PUNKT191 – Marketing und Design  
www.punkt191.de

**BILDNACHWEIS TITEL** Bild generiert mit KI

**VERÖFFENTLICHUNG** Juli 2026





↑ Bild generiert mit KI

Cyberangriffe, Phishing-Mails und verschlüsselte Daten sind längst keine abstrakten Gefahren mehr. Auch kleine und mittlere Unternehmen im Erzgebirge spüren, dass digitale Sicherheit zur Grundlage stabiler Geschäftsprozesse geworden ist. Praxisbeispiele aus der Region zeigen: IT-Sicherheit beginnt nicht erst im Ernstfall – sondern mit Aufmerksamkeit, Vorbereitung und der Bereitschaft, sich Unterstützung zu holen.

sendet, Löhne ausgezahlt, Kundendaten geschützt und Lieferketten aufrechterhalten werden können. Je komplexer digitale Lösungen sind, desto schwerer wird es, sie im Detail zu verstehen und desto größer werden Ängste vor Schäden in Größenordnungen, die man selbst nicht mehr beherrschen und beeinflussen kann. Unternehmen unterschiedlicher Branchen und Größen beschäftigen sich zunehmend mit der Frage, wie sie sich vor Cyberangriffen schützen können.

## IT-Sicherheit im Erzgebirge: Vom Randthema zur Daueraufgabe

Die Unternehmen im Erzgebirge stehen für industrielle Stärke, handwerkliche Präzision, internationale Kundenbeziehungen und Innovationskraft. Viele Betriebe haben in den vergangenen Jahren stark in Digitalisierung investiert: Produktionsprozesse wurden vernetzt, Verwaltungsabläufe digitalisiert, Kundendatenbanken aufgebaut, Online-Kommunikation professionalisiert und neue Softwarelösungen eingeführt. Was für Effizienz, Geschwindigkeit und Wettbewerbsfähigkeit sorgt, vergrößert zugleich die digitale Angriffsfläche.

Damit rückt ein Thema stärker in den Mittelpunkt, das lange eher als Spezialgebiet einzelner IT-Verantwortlicher galt: IT-Sicherheit. Heute betrifft IT-Sicherheit nahezu alle Bereiche eines Unternehmens. Sie entscheidet mit darüber, ob Angebote geschrieben, Maschinen gesteuert, Rechnungen ver-

## IT-Sicherheit als regionale Herausforderung für kleine und mittlere Unternehmen

Cyberkriminalität trifft nicht nur internationale Konzerne oder große öffentliche Einrichtungen. Gerade die Gefahr für kleine und mittlere Unternehmen wird häufig unterschätzt. Die Annahme, für Angreifende nicht interessant genug zu sein, ist riskant. Viele Angriffe erfolgen automatisiert. Dabei wird nicht zuerst gefragt, ob ein Unternehmen prominent oder groß ist, sondern ob es verwundbare Systeme, schwache Passwörter, ungepatchte Software oder unaufmerksame Nutzende gibt.

Das zeigt sich auch in den Rückmeldungen aus der Region. Bei mehreren Unternehmen ist die Wahrnehmung ähnlich: Das Thema wird präsenter. Gleichzeitig wächst der Wunsch, eigene Strukturen prüfen zu lassen, Mitarbeitende zu sensibilisieren und im Ernstfall schneller reagieren zu können. Für



den Mittelstand und besonders für Kleinunternehmen ist das herausfordernd. Viele Betriebe verfügen nicht über große IT-Abteilungen und oft tragen einzelne Verantwortliche mehrere Aufgaben gleichzeitig. Externe Dienstleistende unterstützen zwar, doch strategische Entscheidungen zur IT-Sicherheit müssen trotzdem im Unternehmen selbst getroffen werden. Genau hier setzt das **Mittelstand-Digital Zentrum Chemnitz** an: mit Informationen, Veranstaltungen, individuellen Gesprächen und Impulsprojekten, die konkrete Bedarfe der Unternehmen aufgreifen.

## IT-Sicherheit mit System: Die Perspektive des Mittelstand-Digital Zentrum Chemnitz

Roland Hallau vom Mittelstand-Digital Zentrum Chemnitz begleitet das Thema IT-Sicherheit seit vielen Jahren. Bereits seit 2018 gehört es zum festen Angebot des Zentrums. Aus seiner Sicht haben sich viele Grundfragen nicht verändert: Unternehmen benötigen verlässliche Datensicherungen, klare Authentifizierungsverfahren, ein aktuelles Update- und Patch-Management sowie eine kontinuierliche Sensibilisierung der Mitarbeitenden.

Verändert hat sich jedoch die Bedrohungslage. Phishing und Ransomware zählen zu den typischen Risiken, mit denen kleine und mittlere Unternehmen konfrontiert sind. Bei Ransomware werden Daten verschlüsselt, Systeme blockiert oder Unternehmen erpresst. Phishing wiederum zielt darauf ab, Zugangsdaten zu erlangen, Zahlungen umzuleiten oder Schadsoftware einzuschleusen. Besonders problematisch ist, dass solche Angriffe durch Künstliche Intelligenz professioneller werden können. Gefälschte Nachrichten wirken sprachlich überzeugender, schneller erstellt und schwerer zu erkennen.

Hallau beschreibt IT-Sicherheit deshalb als Basis jeder Digitalisierung. Wer digitale Prozesse einführt, muss diese Prozesse auch absichern. Das gilt für klassische Büro-IT genauso wie für Produktionssysteme, digitale Kundenkommunikation oder KI-Anwendungen. IT-Sicherheit ist damit kein nachträglicher Zusatz, sondern Voraussetzung für einen stabilen unternehmerischen Alltag. „Man kann sagen, dass sich die Gefährdungen direkt (mindestens) proportional zum Digitalisierungsgrad (inkl. KI) entwickeln werden“, so Hallau.

## IT-Sicherheit bei Brandes Technik: Vorsorge statt falscher Sicherheit

Die Brandes Technik GmbH steht beispielhaft für Unternehmen, die bisher keinen konkreten Cyberangriff erlebt haben, das Thema aber dennoch ernst nehmen. Entsprechend gewinnt laut eigener Aussage auch hier Prävention, Sensibilisierung und der Schutz der IT-Infrastruktur kontinuierlich an Bedeutung, heißt es aus dem Unternehmen.

Aus Sicht des Kunststoffverarbeiters zeigen die zunehmende Digitalisierung und steigende Zahl an Cyberangriffen deutlich, dass sich Betriebe nicht in trügerischer Sicherheit wiegen sollten. Denn, so Geschäftsführer Volker Schreiter: „Aus unserer Sicht stellt sich heute nicht mehr die Frage, ob ein Unternehmen mit diesen Risiken konfrontiert wird, sondern vielmehr wann.“

Die Zusammenarbeit mit dem Mittelstand-Digital Zentrum Chemnitz war für das Unternehmen eine Möglichkeit, erste Schritte in einem komplexen Themenfeld zu gehen. Besonders wichtig waren dabei kompetente Ansprechpersonen und eine praxisnahe Unterstützung. Denn viele mittelständische Unternehmen wissen zwar, dass IT-Sicherheit wichtig ist, stehen aber vor der Frage, wo sie anfangen sollen. Geht es zuerst um Backups? Um Passwörter? Um Netzwerkstrukturen? Um Dienstleistende? Oder um Schulungen?

## IT-Sicherheit bei Wittigsthal TGA Solutions: Netzwerk prüfen und Mitarbeitende stärken

Auch die Wittigsthal TGA Solutions GmbH misst IT-Sicherheit eine große Bedeutung zu und sieht, dass die Intensität von Angriffen zunimmt. Einen konkreten Sicherheitsvorfall gab es nach Unternehmensangaben bisher nicht. Dennoch wurde im Rahmen der Zusammenarbeit mit dem Mittelstand-Digital Zentrum Chemnitz die Sicherheitsarchitektur des Netzwerks überprüft. Solche Analysen sind für Unterneh-



men besonders wertvoll, weil sie einen strukturierten Blick von außen ermöglichen. Ein weiterer Schwerpunkt war die Sensibilisierung der Mitarbeitenden. Dieser Punkt ist zentral, denn IT-Sicherheit entscheidet sich nicht allein an technischen Schutzmaßnahmen. Mitarbeitende öffnen E-Mails, vergeben Passwörter, greifen aus dem Homeoffice auf Systeme zu, nutzen mobile Geräte und reagieren auf Anfragen von außen oder vermeintlichen Vorgesetzten.

Betriebswirt Gerald Jonas, welcher vonseiten der Wittigsthal TGA Solutions mit dem Digitalzentrum Chemnitz zusammengearbeitet hat, rät anderen Unternehmen aus der Region deshalb: „Das Angebot des Mittelstand-Digital Zentrums in Anspruch zu nehmen und nicht darauf zu vertrauen, wir seien doch uninteressant oder zu klein. [...] jedes Unternehmen kann es treffen und dann sollte man vorbereitet sein.“

## IT-Sicherheit bei Wendt & Kühn: Wenn Phishing zur realen Erfahrung wird

Auch Peter Schuricht von Wendt & Kühn teilt diese Einschätzung: „Die Gefahr durch Cyberkriminalität sollte keinesfalls unterschätzt werden. Das Argument „Wir sind nur ein kleines Unternehmen. Wieso sollte jemand uns angreifen?“ steht einer wachsenden Zahl an Angriffen auf kleine und mittlere Unternehmen gegenüber.“

Auch wenn IT-Sicherheit in den meisten Unternehmen oftmals nur Mittel zum Zweck ist: Wenn man die eigene IT-Sicherheit vernachlässigt, „[...] muss man sich auf das Glück verlassen, nicht Ziel eines Hackerangriffes zu werden.“

Zwei Phishing-Angriffe auf das traditionsreiche Unternehmen zeigen, wie schnell aus einer abstrakten Bedrohung ein konkreter Vorfall werden kann. Das Vorgehen der Angreifer zeigte ein klassisches Muster: der Versuch, Zugangsdaten von internen Nutzerkonten zu erlangen, um dann über diese Konten anschließend weitere Phishing-Mails zu versenden, um zusätzliche Zugangsdaten zu erlangen und den Angriff so auszubreiten.

Phishing-Attacken sind insbesondere gefährlich, weil sie auf alltäglich genutzte Kommunikationswege wie E-Mails und Webseiten setzen. Gerade im Arbeitsalltag genügt oft ein kurzer Moment der Unachtsamkeit: Eine Nachricht wirkt ver-

traut, ein Link führt auf eine täuschend echte Website und eine scheinbar legitime Anmeldemaske fordert zur Eingabe sensibler Zugangsdaten auf.

Wendt & Kühn zog klare Konsequenzen. Eine wichtige Maßnahme war die Einführung von Multifaktor-Authentifizierung. Sie sorgt dafür, dass ein Passwort allein nicht ausreicht, um Zugriff zu erhalten. Ebenso wichtig ist die Schulung der Mitarbeitenden im Umgang mit verdächtigen E-Mails. Dabei geht es nicht darum, Beschäftigte zu verunsichern, sondern sie handlungsfähig zu machen.

In einem anstehenden Impulsprojekt mit dem Mittelstand-Digital Zentrum Chemnitz plant Wendt & Kühn zudem eine Schwachstellenanalyse der IT-Infrastruktur. Dabei sollen externe und interne Bereiche betrachtet, mögliche Sicherheitslücken identifiziert und behoben werden. Zudem soll ein sogenannter IT-Notfallplan entstehen.

## IT-Sicherheit durch Notfallplanung: Vorbereitung auf den Ernstfall

Ein IT-Notfallplan ist für viele Unternehmen ein entscheidender Schritt. Denn selbst die besten Schutzmaßnahmen können keinen vollständigen Schutz garantieren. Ein Notfallplan legt fest, wer informiert wird, welche Systeme priorisiert werden, welche externen Partner einbezogen werden und wie die Kommunikation abläuft. Dazu gehört auch die Frage, wie schnell Daten wiederhergestellt werden können. Backups sind nur dann hilfreich, wenn sie regelmäßig erstellt, sicher gespeichert und praktisch getestet werden. Unternehmen sollten wissen, wie lange eine Wiederherstellung dauert und welche Daten im Notfall zuerst benötigt werden. Ebenso wichtig ist die Dokumentation. Wenn nur einzelne Personen wissen, wie Systeme aufgebaut sind oder wo Zugangsdaten verwaltet werden, entsteht ein zusätzliches Risiko. IT-Sicherheit bedeutet deshalb auch, Wissen im Unternehmen verfügbar zu machen und klare Zuständigkeiten zu schaffen.

Wichtig ist: IT-Sicherheit darf nicht allein an IT-Verantwortliche delegiert werden. Sie ist eine Führungsaufgabe.



# IT-Sicherheit mit Unterstützung: Impulse für die Region

Am Ende geht es nicht nur um Technik. Es geht um die Sicherung des unternehmerischen Alltags. Für den Mittelstand im Erzgebirge ist IT-Sicherheit damit ein wesentlicher Baustein von Resilienz und ein Thema, das dauerhaft auf die Agenda gehört.

Die Beispiele von Brandes Technik, Wittigsthal TGA Solutions und Wendt & Kühn zeigen, dass das Thema IT-Sicherheit im Erzgebirge angekommen ist. Die Ausgangslagen sind unterschiedlich: Manche Unternehmen waren bisher nicht betroffen, andere haben bereits konkrete Erfahrungen mit Phishing gemacht. Gemeinsam ist ihnen die Erkenntnis, dass Abwarten und Hoffen keine Strategien sind.

Das Mittelstand-Digital Zentrum Chemnitz bietet dafür einen niedrigschwelligen Zugang. Veranstaltungen sensibilisieren, Publikationen geben Orientierung und Impulsprojekte ermöglichen praktische Schritte. Für Unternehmen, die bisher unsicher sind, wo sie beginnen sollen, kann genau dieser Einstieg entscheidend sein.

## IT-Sicherheit als Voraussetzung für Zukunftsfähigkeit

Digitalisierung, Automatisierung und Künstliche Intelligenz werden die Wirtschaft weiter verändern. Damit wächst auch die Verantwortung, digitale Prozesse sicher zu gestalten. IT-Sicherheit ist deshalb kein Bremsklotz für Innovation, sondern ihre Voraussetzung. Nur wer Systeme schützt, Daten verfügbar hält und Mitarbeitende vorbereitet, kann digitale Möglichkeiten verlässlich nutzen.

Die zentrale Botschaft aus den Praxisbeispielen lautet: Unternehmen sollten IT-Sicherheit nicht aufschieben. Der Einstieg muss nicht perfekt sein, aber er sollte beginnen. Eine erste Analyse, ein Gespräch mit Fachleuten, eine Schulung oder die Einführung von Multifaktor-Authentifizierung können wichtige Schritte sein.



## Verfasst von

**MARCUS SCHÖNFELD** ist Projektmanager bei der Wirtschaftsförderung Erzgebirge im Geschäftsbereich Wirtschaftsservice mit den Schwerpunkten Innovation und Digitalisierung. Im Mittelstand-Digital Zentrum Chemnitz agiert er als Transferpartner.. [marcus.schoenfeld@digitalzentrum-chemnitz.de](mailto:marcus.schoenfeld@digitalzentrum-chemnitz.de)

## Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

### **WAS IST MITTELSTAND-DIGITAL?**

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. 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 der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter [www.mittelstand-digital.de](http://www.mittelstand-digital.de).



Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

aufgrund eines Beschlusses  
des Deutschen Bundestages

Mittelstand-Digital 