Mittelstand-Digital
Zentrum
Spreeland

Cybersicherheit im Mittelstand

Mehr als nur Schutz

www.digitalzentrum-spreeland.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital

Disclaimer:
Diese Broschüre wirbt nicht für spezifische Hard- oder Software.
Dargestellte Inhalte werden ausschließlich zur Veranschaulichung der Einsatzmöglichkeiten genutzt.

Cybersicherheit im Mittelstand:

Mehr als nur Schutz

„Cybersicherheit in kleinen und mittleren Unternehmen (KMU) ist mehr als Schutz – sie sichert Stabilität, Vertrauen und fördert Innovation sowie Wachstum durch sichere IT-Infrastrukturen. In einer vernetzten digitalen Welt ist sie ein entscheidender Erfolgsfaktor.“

Mit der fortschreitenden digitalen Transformation wird Cybersicherheit zu einer der größten Herausforderungen für den deutschen Mittelstand. Die Digitalisierung bietet enorme Chancen, erhöht jedoch auch das Risiko von Cyberangriffen und Datenverlusten, die nicht nur den Geschäftsbetrieb, sondern auch das Vertrauen von Kunden und Partnern gefährden. In dieser Broschüre erfahren Sie, wie Sie Cybersicherheit als Wettbewerbsvorteil nutzen können und wie Sie Bedrohungen erfolgreich abwehren, um eine zukunftssichere Grundlage für Ihr Unternehmen zu schaffen.

Diese Broschüre bietet einen Überblick über:

- Das Phänomen Cybersicherheit:
  Warum ist sie für KMU so wichtig?
- Grundlagen der IT-Sicherheit:
  Essenzielle Bausteine für Schutz und Resilienz.
- IIoT-Sicherheit:
  Herausforderungen und Schutzstrategien für vernetzte Produktionssysteme.
- Vorteile und Anwendungen:
  Wie KMU von effektiver Cybersicherheit profitieren.
- Leitfaden zur Umsetzung:
  Schritt für Schritt zu einer sicheren IT-Umgebung.
- Wie deutsche KMU ihre Cybersicherheit stärken:
  Erfolgreiche Beispiele.
- Cybersicherheit in der Praxis:
  Mit Fischertechnik zum Schutz Ihres Unternehmens.

Das Phänomen Cybersicherheit:

Warum ist sie für KMU so wichtig?

Cybersicherheit ist weit mehr als eine technische Notwendigkeit – sie ist ein unverzichtbarer Erfolgsfaktor für KMU. Die zunehmende Digitalisierung und Vernetzung bieten immense Chancen, schaffen jedoch auch neue Angriffsflächen für Cyberkriminelle. Diese Bedrohungen gefährden nicht nur den Geschäftsbetrieb, sondern können auch das Vertrauen von Kunden und Partnern untergraben.

Verfügbarkeit digitaler Infrastrukturen

Vernetzung: Die digitale Vernetzung von KMU beschleunigt Geschäftsprozesse, eröffnet jedoch auch neue Angriffspunkte für Cyberkriminelle. **Cloud-Dienste:** Cloud-Lösungen bieten erhebliche Vorteile, müssen jedoch mit geeigneten Schutzmaßnahmen gesichert werden, um Datenverluste oder unbefugten Zugriff zu verhindern.

Zunahme von Cyberangriffen

Anstieg der Bedrohungen: Laut einer Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) richten sich 43 % der Cyberangriffe gegen KMU, da diese oft unzureichend geschützt sind (Quelle: BSI, 2023). **Finanzielle Auswirkungen:** Ein erfolgreicher Angriff kann erhebliche Kosten verursachen. Der durchschnittliche Schaden durch einen Cyberangriff beträgt für KMU etwa 200.000 € (Quelle: Hiscox, 2022).

Schutz von Kunden- und Geschäftsdaten

Verantwortung: Der Schutz sensibler Daten ist entscheidend für das Vertrauen von Kunden und Partnern. 70 % der Verbraucher geben an, dass sie Unternehmen wechseln würden, wenn ihre Daten nicht sicher sind (Quelle: Kaspersky, 2022). **Datenschutz:** Die Einhaltung von Datenschutzvorschriften wie der DSGVO ist nicht nur gesetzlich vorgeschrieben, sondern schützt Unternehmen auch vor hohen Bußgeldern (Quelle: Europäische Kommission, 2021).

Verfügbarkeit und Schutz von IT-Ressourcen

Komplexität: Mit zunehmender IT-Komplexität wächst der Bedarf an robusten Sicherheitsmaßnahmen, um die Kontrolle über IT-Systeme zu behalten. **Zukunftssicherheit:** Cybersicherheit stellt sicher, dass IT-Ressourcen in einer zunehmend komplexen und vernetzten Welt widerstandsfähig bleiben.

Grundlagen der IT-Sicherheit:

Wesentliche Bausteine für Schutz und Resilienz

IT-Sicherheit schützt Unternehmen vor Bedrohungen und Angriffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen zu gewährleisten. Sie umfasst verschiedene Maßnahmen, die sich auf Netzwerke, Daten, Endgeräte, Identitäten und Zugriffe beziehen.

Wichtige Bausteine der IT-Sicherheit:

Netzwerksicherheit: Der Schutz von Netzwerken vor unbefugtem Zugriff erfolgt durch Firewalls, Intrusion Detection Systems (IDS) und VPN-Technologien.

Endgerätesicherheit: Mit Antiviren-Software und Mobile Device Management (MDM) schützen Sie Endgeräte wie PCs, Smartphones und Tablets.

Mitarbeitersensibilisierung: Regelmäßige Schulungen und klare Sicherheitsrichtlinien verringern das Risiko menschlicher Fehler.

Datensicherheit: Die Verschlüsselung von Daten und regelmäßige Backups schützen vor Datenverlust und unbefugtem Zugriff.

Identitäts- und Zugriffsmanagement: Multi-Faktor-Authentifizierung (MFA) und starke Passwörter verhindern unbefugten Zugriff.

Kontinuierliche Verbesserung: Regelmäßige Audits und eine Notfallstrategie helfen, bei einem Angriff schnell zu reagieren und den Betrieb rasch wiederherzustellen.

IIoT-Sicherheit:

Herausforderungen und Schutzstrategien für vernetzte Produktionssysteme

Die Einführung von Industrie-4.0-Technologien und des Industrial Internet of Things (IIoT) hat die Produktionslandschaft revolutioniert. Sie bietet erhebliche Vorteile in Bezug auf Effizienz und Innovation, bringt jedoch auch neue Sicherheitsherausforderungen mit sich. Veraltete Infrastrukturen und unzureichende Schutzmaßnahmen machen Produktionssysteme anfällig für Cyberangriffe wie Manipulation, Malware oder Ransomware. Die zentrale Bedrohung besteht in der Gefährdung der Verfügbarkeit, Vertraulichkeit und Integrität dieser Systeme.

Abbildung 1 Simulation zur Cybersicherheit in einem IIoT-System

Ein besonders hohes Risiko entsteht durch die Vielzahl an vernetzten Geräten, die in Produktionsumgebungen genutzt werden. Viele dieser Geräte verfügen nicht über integrierte Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung. Hinzu kommt, dass die Integration von IIoT-Technologien in bestehende Produktionsinfrastrukturen häufig Sicherheitslücken offenbart, da ältere Systeme ursprünglich nicht für eine vernetzte Umgebung ausgelegt waren. Ein Mangel an klar definierten Sicherheitsstrategien und die unzureichende Schulung von Mitarbeitern erhöhen das Risiko zusätzlich.

Schutzmaßnahmen für IIoT-Systeme

Um diesen Herausforderungen zu begegnen, benötigen Unternehmen eine ganzheitliche Sicherheitsstrategie für ihre IIoT-Umgebungen. Wesentliche Schutzmaßnahmen umfassen:

- **Netzwerksegmentierung**
  Kritische Produktionssysteme sollten von weniger sensiblen IT-Systemen getrennt werden, um die Ausbreitung potenzieller Angriffe zu minimieren.

- **Kontinuierliche Überwachung und Anomalieerkennung**
  Die Analyse von Datenströmen und Systemaktivitäten auf ungewöhnliche Muster kann potenzielle Angriffe frühzeitig erkennen und entsprechende Gegenmaßnahmen ermöglichen.

- **Endpoint-Security**
  Jedes IIoT-Gerät stellt ein potenzielles Einfallstor für Angreifer dar. Daher sind sichere Authentifizierungsverfahren wie Zertifikats-basierte Authentifizierung und Multi-Faktor-Authentifizierung (MFA) unverzichtbar.

- **Regelmäßiges Patch-Management**
  Sicherheitslücken in Geräten und Systemen sollten durch regelmäßige Updates und Patches geschlossen werden.

- **Verschlüsselungstechnologien**
  Die Kommunikation zwischen Geräten, Steuerungssystemen und Cloud-Plattformen sollte durch Verschlüsselung geschützt werden, um unbefugten Zugriff und Manipulationen zu verhindern.

- **Notfallplanung**
  Ein klar definierter Notfallplan ermöglicht schnelle Reaktionszeiten im Falle eines Angriffs, minimiert Schäden und gewährleistet die schnelle Wiederaufnahme der Produktion.

- **Schulung und Sensibilisierung der Mitarbeiter**
  Menschliches Fehlverhalten zählt zu den Hauptursachen für Sicherheitslücken. Regelmäßige Schulungen zu Themen wie Phishing-Schutz und Social Engineering fördern das Bewusstsein für Cybersicherheit und helfen, Angriffsrisiken zu reduzieren.

Durch die Umsetzung dieser Maßnahmen können Unternehmen ihre vernetzten Produktionssysteme effektiv vor Bedrohungen schützen. Dies ermöglicht es, die Vorteile von IIoT-Technologien voll auszuschöpfen, während Sicherheit und Effizienz Hand in Hand gehen – eine Grundlage für nachhaltige und zukunftsfähige Produktionsprozesse.

Vorteile und Anwendungen:

Wie KMU von effektiver Cybersicherheit profitieren

Effektive Cybersicherheit schützt KMU nicht nur vor Bedrohungen, sondern fördert auch Innovation und Wettbewerbsfähigkeit. Sie bietet zahlreiche Vorteile und Anwendungen, die Unternehmen helfen, in einer digitalen Welt sicher und erfolgreich zu bleiben.

Schutz vor Cyberangriffen

Ziel: Abwehr von Bedrohungen wie Ransomware und Phishing.

Vorteil: Minimierung von Systemausfällen und Datenverlusten.

Beispiel: Firewalls und regelmäßige Updates helfen, Angriffe frühzeitig zu erkennen.

Kostenreduzierung durch Prävention

Ziel: Senkung der Kosten durch präventive Maßnahmen.

Vorteil: Vermeidung von teuren Ausfallzeiten und Reparaturen.

Beispiel: Proaktive Sicherheitsmaßnahmen verhindern kostspielige Angriffe.

Verbesserung der Geschäftsresilienz

Ziel: Sicherstellung der Betriebsfähigkeit bei Angriffen.

Vorteil: Schnelle Wiederherstellung von Systemen und Daten.

Beispiel: Cloud-Backups ermöglichen eine rasche Wiederherstellung nach einem Angriff.

Verbesserung der Wettbewerbsfähigkeit

Ziel: Positionierung als sicheres und vertrauenswürdiges Unternehmen.

Vorteil: Eröffnung neuer Geschäftsmöglichkeiten.

Beispiel: Sichere digitale Lösungen ermöglichen effiziente Zusammenarbeit.

Stärkung des Kundenvertrauens

Ziel: Schutz von Kunden- und Unternehmensdaten.

Vorteil: Steigerung des Vertrauens von Kunden und Partnern.

Beispiel: Einhaltung der DSGVO stärkt das Vertrauen in den Datenschutz.

Förderung von Innovation und Wachstum

Ziel: Schaffung einer sicheren Grundlage für digitale Innovation.

Vorteil: Erschließung neuer Geschäftsmodelle.

Beispiel: Sichere Cloud-Dienste unterstützen flexible, innovative Geschäftslösungen.

Leitfaden zur Umsetzung:

Schritt für Schritt zur sicheren IT-Umgebung

Die Umsetzung einer sicheren IT-Umgebung ist für KMU entscheidend, um Systeme und Daten vor Cyberbedrohungen zu schützen. Ein strukturierter Ansatz hilft, Risiken zu minimieren und die IT-Infrastruktur resilient zu machen.

Sicherheitsanalyse & Risikobewertung

Ziel: Identifikation von Schwachstellen.
Vorteil: Präzise Risikoanalyse zeigt gefährdete Bereiche.
Beispiel: Durchführung von Penetrationstests zur Früherkennung von Schwachstellen.

Firewall & Intrusion Detection Systems

Ziel: Schutz vor unbefugtem Zugriff.
Vorteil: Verhindert Hackerangriffe.
Beispiel: Einrichtung von Firewalls und IDS zur Erkennung verdächtiger Aktivitäten.

Daten-verschlüsselung

Ziel: Schutz von vertraulichen Daten.
Vorteil: Verhindert das Abfangen von Informationen.
Beispiel: Verschlüsselung von E-Mails und Datenbanken.

Multi-Faktor-Authentifizierung (MFA)

Ziel: Verstärkung des Zugriffsmanagements.
Vorteil: Erschwert unbefugten Zugriff.
Beispiel: Aktivierung von MFA für alle geschäftlichen Anwendungen.

Regelmäßige Updates & Patch-Management

Ziel: Schließung von Sicherheitslücken.
Vorteil: Verhindert Ausnutzung von Schwachstellen.
Beispiel: Automatische Software-Updates für Betriebssysteme und Anwendungen.

Schulung der Mitarbeiter

Ziel: Minimierung von Risiken durch menschliches Versagen.
Vorteil: Erhöhtes Bewusstsein für Sicherheitsbedrohungen.
Beispiel: Regelmäßige Phishing-Tests und Sicherheitsschulungen.

Wie deutsche KMU ihre Cybersicherheit stärken:

Erfolgreiche Beispiele

Deutsche KMU haben in den letzten Jahren ihre Cybersicherheitsmaßnahmen erheblich verbessert, indem sie fortschrittliche Lösungen eingeführt haben, die speziell auf ihre Bedürfnisse zugeschnitten sind. Hier sind einige Beispiele, wie KMU ihre Abwehrkräfte gegen Cyberbedrohungen ausgebaut haben:

1. **E-Commerce KMU setzen auf proaktive Sicherheitsmaßnahmen:**

   Viele Online-Händler haben robuste Sicherheitsprotokolle wie Firewalls und MFA implementiert, um Phishing-Versuche und unbefugte Zugriffe abzuwehren. Regelmäßige Software-Updates und Mitarbeiterschulungen gehören ebenfalls zum Standard, um die allgemeine Sicherheit weiter zu stärken.

   Ergebnis: Diese Maßnahmen haben den Schutz von Kundendaten und Zahlungsinformationen gewährleistet, Vertrauen geschaffen und zu stabilen Umsätzen geführt.

2. **KMUs im Rechtssektor schützen sensible Mandantendaten:**

   Im Rechtssektor haben KMU große Fortschritte beim Schutz sensibler Mandantendaten gemacht, indem sie Kommunikation verschlüsseln und regelmäßige Backups sowie kontinuierliche Monitoring-Systeme eingeführt haben. Diese Maßnahmen haben sich als äußerst effektiv im Umgang mit Bedrohungen wie Ransomware erwiesen.

   Ergebnis: Die Geschäftsabläufe konnten ohne Unterbrechung fortgesetzt werden, und die Vertraulichkeit der Mandantendaten blieb gewahrt, was das Vertrauen in das Unternehmen weiter stärkte.

3. IT-Dienstleister führen umfassende Cybersicherheits-Audits durch:

IT-Dienstleister haben Sicherheitslücken frühzeitig erkannt, indem sie gründliche Sicherheitsanalysen durchgeführt und mehrstufige Schutzsysteme eingeführt haben. Dazu gehören Maßnahmen wie Penetrationstests, IDS und Netzwerksegmentierung zur Risikominimierung.

Ergebnis: Diese Strategien haben teure Datenpannen und Systemausfälle verhindert und das Vertrauen der Kunden durch transparente Sicherheitspraktiken gestärkt.

4. Fertigungsunternehmen sichern ihre Produktion durch Cybersicherheit:

Fertigungsunternehmen haben Cybersicherheitsmaßnahmen in ihren Produktionsalltag integriert, indem sie Systeme zur Anomalieerkennung und Netzwerksegmentierung eingeführt haben, um die Produktion auch bei Cyberbedrohungen aufrechtzuerhalten.

Ergebnis: Diese proaktiven Maßnahmen haben es ermöglicht, gezielte Cyberangriffe abzuwehren und die Produktion ohne Unterbrechung fortzuführen.

5. Finanzdienstleister setzen auf Cloud-Sicherheit:

Finanzdienstleister haben fortschrittliche Cloud-Sicherheitslösungen eingeführt, um sensible Finanzdaten zu schützen. Diese Lösungen, ergänzt durch Echtzeitüberwachung und Verschlüsselung, bieten einen robusten Schutz vor Cyberbedrohungen und ermöglichen eine sichere Kontrolle des Zugriffs auf wichtige Systeme.

Ergebnis: Mit verbesserter Cloud-Sicherheit haben diese KMU die Integrität sensibler Daten gewahrt, Cyberangriffe erfolgreich abgewehrt und langfristiges Kundenvertrauen gestärkt.

Diese Beispiele zeigen, wie deutsche KMU ihre Cybersicherheit kontinuierlich verbessern, um ihre Geschäftsprozesse zu schützen, sensible Informationen zu sichern und das Vertrauen ihrer Kunden zu erhalten. Durch proaktive Maßnahmen und den Einsatz innovativer Lösungen sind diese Unternehmen bestens gerüstet, um den sich ständig wandelnden Cyberbedrohungen zu begegnen.

Cybersicherheit in der Praxis:

Mit Fischertechnik zum Schutz Ihres Unternehmens

Als Mittelstand-Digital Zentrum Spreeland bieten wir umfassende Workshops und Vorträge zur Cybersicherheit für KMU an, bei denen unser Fischertechnik Demonstrator zum Einsatz kommt.

Dieser Demonstrator dient als interaktive Plattform zur Simulation und Visualisierung von Cybersicherheitsmaßnahmen in einer Unternehmensumgebung, insbesondere im Zusammenhang mit IoT und vernetzten Geräten.

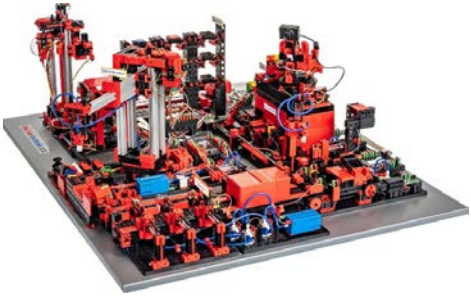

Abbildung 2 Fischertechnik Lernfabrik 4.0

Ein zentraler Bestandteil des Demonstrators ist die Verwendung des MQTT-Protokolls (Message Queuing Telemetry Transport), eines weit verbreiteten Kommunikationsprotokolls, das besonders in IoT-Umgebungen genutzt wird. MQTT ist aufgrund seiner Leichtgewichtigkeit und Effizienz sehr beliebt, birgt jedoch auch eine Reihe von Sicherheitsrisiken. In seiner Standardform bietet MQTT keine Verschlüsselung und keine Authentifizierung, was es anfällig für Angriffe macht.

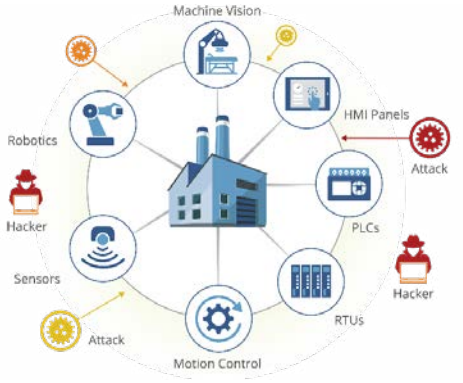

Abbildung 3 Angriffe auf IIoT-Systeme

Angreifer können MQTT-Nachrichten abhören (Eavesdropping) oder manipulieren (Man-in-the-Middle-Angriffe), insbesondere wenn diese über unsichere Netzwerke übertragen werden. Ein weiteres häufiges Sicherheitsproblem bei MQTT ist das Fehlen einer strikten Authentifizierung. Ohne geeignete Authentifizierungsmechanismen könnten Angreifer unbefugten Zugriff auf das IoT-System erlangen, Nachrichten verfälschen oder Geräte steuern. Zudem können Angreifer Denial-of-Service (DoS)-Angriffe durchführen, bei denen sie den Broker überlasten und die Kommunikation zwischen den Geräten unterbrechen.

Im Rahmen unserer Workshops und Vorträge demonstrieren wir, wie diese Sicherheitslücken in einem Unternehmensnetzwerk ausgenutzt werden können und zeigen, wie Cybersicherheitslösungen implementiert werden können, um diese Gefahren zu minimieren. Dazu gehören:

1. **Verschlüsselung von MQTT-Nachrichten:** Durch den Einsatz von SSL/TLS können alle über MQTT übertragenen Daten verschlüsselt werden, sodass sie für Angreifer unlesbar werden.

2. **Authentifizierung und Autorisierung:** Wir erklären, wie MQTT-Server so konfiguriert werden können, dass nur autorisierte Clients Zugriff auf die Daten haben. Dies kann durch die Implementierung von Benutzernamen und Passwort oder durch sicherere Methoden wie Zertifikats-basierte Authentifizierung erfolgen.

3. **Zertifikats-basierte Kommunikation:** Eine sichere MQTT-Kommunikation erfordert die Verwendung von X.509-Zertifikaten, um die Identität von Clients und Servern zu überprüfen und sicherzustellen, dass die Verbindung zwischen den Geräten authentifiziert ist.

4. **Zugangskontrollen:** Wir zeigen, wie Unternehmen ihre IoT-Geräte und Netzwerke segmentieren können, sodass nur berechtigte Geräte miteinander kommunizieren können und unautorisierte Geräte keinen Zugriff auf kritische Netzwerke oder Daten erhalten.

5. **Überwachung und Logging:** Eine kontinuierliche Überwachung und das Sammeln von Logs ermöglichen es, verdächtige Aktivitäten frühzeitig zu erkennen und schnell auf potenzielle Sicherheitsvorfälle zu reagieren.

In diesen Workshops erfahren KMU, wie sie durch den Einsatz dieser Sicherheitslösungen ihre Systeme vor Angriffen schützen und eine widerstandsfähige IT-Infrastruktur aufbauen können. Die praxisnahe Demonstration von Angriffen zeigt, wie diese Schwachstellen in einer realen Umgebung ausgenutzt werden könnten und wie durch gezielte Sicherheitsmaßnahmen das Risiko erheblich reduziert werden kann.

Zusätzlich bieten wir unseren Teilnehmenden die Möglichkeit, den Fischertechnik Demonstrator in unserer Modellfabrik zu besuchen.

Dort erhalten sie eine detaillierte Erklärung zur praktischen Umsetzung dieser Sicherheitsmechanismen und können sehen, wie sie in ihrer eigenen Unternehmensumgebung angewendet werden können. Unsere Experten stehen bereit, um auf individuelle Fragen einzugehen und maßgeschneiderte Lösungen für jedes Unternehmen zu entwickeln.

Im Mittelstand-Digital Zentrum Spreeland unterstützen wir KMU nicht nur dabei, die Risiken des MQTT-Protokolls und anderer IoT-Technologien zu verstehen, sondern auch bei der Entwicklung und Umsetzung maßgeschneiderter Cybersicherheitsstrategien. Wir helfen dabei, die IT-Infrastruktur zu optimieren, Sicherheitslücken zu schließen und eine robuste Sicherheitsarchitektur zu implementieren, die sowohl die aktuellen als auch zukünftigen Bedrohungen abwehren kann.

Durch unsere praxisorientierten Workshops und Demonstrationen können KMU ihre digitale Sicherheit erheblich stärken, ihre Netzwerke und Daten schützen und langfristig sicher und erfolgreich in einer zunehmend vernetzten Welt agieren.

Was ist Mittelstand-Digital?

Mit regionalen und thematischen Zentren bietet Mittelstand-Digital im ganzen Bundesgebiet kompetente und anbieterneutrale Anlaufstellen zur Information, Sensibilisierung und Qualifikation: Hier können kleine und mittelständische Unternehmen sowie Handwerksbetriebe durch Praxisbeispiele, Demonstratoren, Informationsveranstaltungen und den gegenseitigen Austausch die Vorteile der Digitalisierung erleben.

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 und stellt finanzielle Zuschüsse bereit.

Was ist das Mittelstand-Digital Zentrum Spreeland?

Das Mittelstand-Digital Zentrum Spreeland unterstützt produzierende kleine und mittlere Unternehmen in Brandenburg und der Lausitz. Durch unser Angebot praxisnaher digitaler Anwendungen, Demonstratoren und Erlebnisräume sowie durch digitale Arbeitsmittel und -prozesse können Unternehmen Innovationskraft entfalten, ihre bestehende Marktpositionen behaupten und weitere Geschäftsfelder und (internationale) Märkte erschließen. Dabei verfolgen wir den Ansatz einer ganzheitlichen digitalen Qualifizierung um Ihr Unternehmen ökonomisch, ökologisch und sozial zukunftsfähig zu machen. Unsere angebotenen Veranstaltungen fördern die Vernetzung mit anderen Unternehmen und unterstützen so die Entwicklung neuer, branchenübergreifender Ideen und Geschäftsmodelle.

Impressum

Herausgeber:
Mittelstand-Digital Zentrum Spreeland
c/o Brandenburgische Technische Universität Cottbus–Senftenberg
Prof. Dr.-Ing. Ulrich Berger
Lehrstuhl Automatisierungstechnik
Siemens-Halske-Ring 14
03046 Cottbus
info@digitalzentrum-spreeland.de
Telefon: +49 355 69-5171

Vertreten durch: Die Brandenburgische Technische Universität Cottbus-Senftenberg ist eine Körperschaft des öffentlichen Rechts und eine staatliche Einrichtung des Landes Brandenburg. Sie wird nach außen durch die Präsidentin, Prof. Dr. Gesine Grande, vertreten.

Zuständige Aufsichtsbehörde: Die BTU Cottbus-Senftenberg untersteht der Rechtsaufsicht des Ministeriums für Wissenschaft, Forschung und Kultur des Landes Brandenburg.

Autor:
Dr.-Ing. Wael Alsabbagh

Satz/Layout:
hyperworx Medienproduktionen
Görlitzer Str. 18
03046 Cottbus

Bildnachweis:
© Canva - Titelseite
© Adobe Stock (3) Freepik (3), iStock (2), ArtemisDiana, Fotomek - Seiten 2, 3
© Inova sense - Seite 4
© Fischertechnik, Veridify Security - Seite 10
© Mittelstand-Digital Zentrum Spreeland - Seite 11

Kontakt

Mittelstand-Digital Zentrum Spreeland
c/o Brandenburgische Technische Universität Cottbus-Senftenberg
Siemens-Halske-Ring 14
03046 Cottbus

Tel.: +49 355 69-5171
info@digitalzentrum-spreeland.de
www.digitalzentrum-spreeland.de

Folgen Sie uns