



**Transferstelle**  
**IT-Sicherheit im Mittelstand**  
Einfach. Sicher. Machen.

# Typisierter Aktionsplan

## Der Weg zu mehr IT-Sicherheit

Szenario „USB-Angriff“



Mittelstand-  
Digital 



Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

## Sehr geehrte:r Besucher:in des ELITE-Erlebnisortes,

zunächst möchten wir Ihnen sagen, dass wir uns sehr freuen, dass Sie an unserem ELITE-Erlebnisort einfache, pragmatische Erzählgeschichten im Demonstrator-Format durchgespielt haben, um sich mit typischen IT-Angriffen und Gefahren im IT-Sicherheitsbereich vertraut zu machen. Das zeigt uns, dass von Seiten der kleinen und mittelständischen Unternehmen tatsächlich ein großes Interesse daran besteht, sich im IT-Sicherheitsbereich weiterzubilden und resilienter für die Zukunft aufzustellen.

An dem **Szenario „USB-Angriff“** haben Sie gesehen, was passieren kann, wenn reale Angriffe gegen Ihr Unternehmen gerichtet werden. Auf diese Situation sind Sie nun besser vorbereitet!

Zu dem am Stand erfolgreich absolvierten Szenario erhalten Sie darüberhinausgehend in diesem Aktionsplan **themenspezifische Aktionen** mit konkreten Umsetzungsvorschlägen für Ihr Unternehmen.

Die in diesem Dokument empfohlenen Aktionen sind in drei Fokusbereiche – organisatorische, technische und personelle Aktionen – gegliedert und passend zu den im Demonstrator adressierten Themen. Damit Sie direkt mit der Umsetzung der Aktionen starten können, gibt es zu jeder Aktion entsprechende Umsetzungsvorschläge. Diese wurden von den IT-Sicherheitsexperten der Projekte Transferstelle IT-Sicherheit im Mittelstand (TISiM, <https://tisim.de>) und ELITE (<https://elite-projekt.de/>) aus dem Angebotskatalog der Transferstelle speziell für das Demonstrator-Szenario ausgewählt.

Über diesen ELITE-Aktionsplan hinausgehend, bietet der Sec-O-Mat (<https://sec-o-mat.de/>) der Transferstelle einem KMU die Möglichkeit, nach Angabe weniger Unternehmenseckdaten, unternehmensspezifische Empfehlungen zu erhalten, basierend auf den konkreten, für das KMU relevante Schadensszenarien.

Wir hoffen, Sie mit dem ELITE-Erlebnisort zur IT-Sicherheit und den darin für Sie bereitgestellten Demonstratoren - und auch mit diesem Aktionsplan - ein Stück sicherer und besser gegenüber Angriffen aus dem Cyberraum wappnen zu können. Wir freuen uns in jedem Fall über Ihre Rückmeldungen jedweder Art unter der Mailadresse [elite-feedback@fraunhofer.de](mailto:elite-feedback@fraunhofer.de).

Wir wünschen Ihnen gute Geschäfte in einer IT-sicheren und gut vorbereiteten Atmosphäre und verbleiben mit freundlichen Grüßen,

Ihr ELITE-Team und Ihre Transferstelle IT-Sicherheit im Mittelstand (TISiM)



# Inhaltsverzeichnis

- **PERS-3: Sicherheitsbewusstsein steigern..... 4**
- **ORG-9: Privatnutzung klären ..... 5**
- **TECH-11: Schadsoftware verhindern ..... 6**
- **ORG-3: Auf IT-Notfälle vorbereiten ..... 7**
- **TECH-3: Datensicherung durchführen und testen..... 8**
- **TECH-2: Sichere Einstellungen wählen..... 9**
- **ORG-2: Überblick über die größten Risiken gewinnen ..... 10**

## ▷ PERS-3: Sicherheitsbewusstsein steigern

---

### 📌 IT-Sicherheit am Arbeitsplatz [Artikel]

**Anbieter:** Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53175 Bonn, Deutschland

**Beschreibung:** Die Checkliste "IT-Sicherheit am Arbeitsplatz" des BSI fasst die wichtigsten Tipps für ein sicherheitsbewusstes Verhalten am digitalen Arbeitsplatz zusammen, um Sicherheitsvorfälle wie Ransomware oder Betrugsversuche zu vermeiden.

**Preis:** kostenlos

**Link:** [IT-Sicherheit am Arbeitsplatz](#)

### 📌 Poster USB-Stick-Alarm

**Anbieter:** KonBriefing, Bahnhofstraße 13, 71696 Möglingen, Deutschland

**Beschreibung:** Mitarbeiter sind ein interessantes Ziel für Kriminelle, die mit verschiedensten und teilweise sehr subtilen Methoden versuchen, Zugriff auf die Unternehmens-IT zu erlangen. Dieses Poster kann dabei helfen, die permanente Bedrohung durch unbekannte USB-Sticks im Bewusstsein zu halten, um im entscheidenden Moment richtig zu reagieren.

**Preis:** kostenlos

**Link:** [Poster USB-Stick-Alarm](#)

### 📌 Themenheft Mittelstand-Digital - Sicherer Datenaustausch [Broschüre/Flyer (Print), Broschüre/Flyer (Digital)]

**Anbieter:** Bundesministerium für Wirtschaft und Klimaschutz, Scharnhorststr. 34-37, 11019 Berlin, Deutschland

**Beschreibung:** Das Themenheft Sicherer Datenaustausch bietet den Lesenden in zehn Artikeln einen Überblick zu verschiedenen Facetten des sicheren Datenaustauschs in Verbindung stehenden Aspekten, wie Online-Datenaustausch, organisatorischen Maßnahmen, Verschlüsselung, dem Faktor Mensch und beispielhaften Anwendungsaspekten. Weiterführende Links verweisen auf zusätzliches Lesematerial zum Thema.

**Preis:** kostenlos

**Link:** [Themenheft Sicherer Datenaustausch](#)

## ▷ ORG-9: Privatnutzung klären

---

### 📄 Leitfaden - Was ist IT-Compliance? [Broschüre/Flyer (Digital)]

**Anbieter:** Mittelstand 4.0-Kompetenzzentrum Planen und Bauen, Fraunhofer Straße 10, 83626 Valley, Deutschland

**Beschreibung:** Das Leitfaden-Dokument „Was ist IT-Compliance?“ bietet eine Einführung in das Thema IT-Compliance an und soll helfen, für Sachverhalte aus dem Bereich der IT-Compliance zu sensibilisieren und damit Problemlagen aus diesem Bereich als solche zu erkennen. Dazu werden mehrere praktische Fallbeispiele gegeben, um mögliche Abläufe im Unternehmen zu identifizieren, in denen Fragenstellungen der IT-Compliance relevant sein können.

**Preis:** kostenlos

**Link:** [Leitfaden – Was ist IT-Compliance?](#)

### 📄 Vortrag von der CeBIT 2013 zu rechtlichen Aspekten von BYOD (Bring Your Own Device) [Video]

**Anbieter:** TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbB, Fasanenstraße 61, 10719 Berlin, Deutschland

**Beschreibung:** In seinem Vortrag von der CeBIT 2013 erläutert Rechtsanwalt Stephan Schmidt von der Kanzlei TCI Rechtsanwälte Mainz die rechtlichen Rahmenbedingungen von BYOD für Unternehmen. In ca. 45 Minuten geht er auf verschiedenste technische und juristische Fragestellungen ein und beleuchtet das Themenfeld sehr umfanglich.

**Preis:** kostenlos

**Link:** [Rahmenbedingungen von BYOD](#)

## ▷ **TECH-11: Schadsoftware verhindern**

---

### 📌 **IT-Sicherheit für KMU [Webinar]**

**Anbieter:** Swisscom AG, Alte Tiefenaustrasse 6, 3050 Bern, Schweiz

**Beschreibung:** In diesem Webinar werden unterschiedliche Arten von Cyberbedrohungen erläutert und dargelegt, was Unternehmen dagegen tun können. Es wird aufgezeigt, wo die größten Sicherheitslücken bei kleinen und mittleren Unternehmen bestehen, welche Folgen Cyberangriffe und Datenverlust nach sich ziehen können und wie KMU sich schützen können. Anschließend werden konkrete Maßnahmen aufgezeigt, wie sich ein KMU vor Verschlüsselungstrojanern schützen kann. Hinweis: Die Aufzeichnung des Webinars muss über ein Online-Formular angefragt werden.

**Preis:** kostenlos

**Link:** [IT-Sicherheit für KMU](#)

### 📌 **Mitarbeiterschulung: Schutz vor Cyber-Kriminalität [Webinar, Präsenzschulung]**

**Anbieter:** IT-Service MEDATA GmbH, Kamphausstr. 4, 49324 Melle, Deutschland

**Beschreibung:** Die IT-Service MEDATA GmbH bietet IT-Sicherheitsschulungen für Mitarbeiter von KMU zum Schutz vor Cyber-Kriminalität an. Die Schulungen werden online via Microsoft Teams oder persönlich vor Ort beim KMU oder in den Schulungsräumlichkeiten des Anbieters durchgeführt.

**Preis:** 140 € (Stunde)

**Link:** [Mitarbeiterschulung: Schutz vor Cyber-Kriminalität](#)

### 📌 **Security Information and Event Management (SIEM): Hackerangriffe erkennen, bevor es zu spät ist**

**Anbieter:** Makro Factory GmbH & Co. KG, An Der RaumFabrik 30, 76227 Karlsruhe, Deutschland

**Beschreibung:** In diesem Artikel wird das Konzept eines SIEM (Security Information and Event Management) erläutert. Als Alternative zu einem klassischen SIEM wird im Artikel das speziell für KMU interessante SIEM-as-a-Service-Modell beschrieben, bei dem die Verantwortlichkeiten für den Aufbau der SIEM-Plattform, den Betrieb und die Pflege beim Dienstleister liegen und somit die Kosten z. B. für Lizenzen, Installation, Beratung und eigene Fachkräfte entfallen. Mit SIEM One stellt der Artikel am Ende eine entsprechende Lösung der Makro Factory vor, die auf einem Virenschanner von ESET basiert.

**Preis:** kostenlos

**Link:** [Artikel zu SIEM](#)

## ▷ ORG-3: Auf IT-Notfälle vorbereiten

---

### 🔗 **Cyber-Sicherheitsnetzwerk - Anlaufstelle und Notfallnummer für Betroffene von IT-Sicherheitsvorfällen**

**Anbieter:** Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53175 Bonn, Deutschland

**Beschreibung:** Das vom BSI seit Ende 2020 aufgebaute Cyber-Sicherheitsnetzwerk (CSN) stellt primär eine Notfall-Telefonnummer und ein entsprechendes Notfall-E-Mail-Postfach also Kontaktstelle für Bürger:innen und Unternehmen nach einem IT-Sicherheitsvorfall bereit. Im Rahmen der Anlaufstelle fungiert das BSI ausschließlich als Vermittler hin zu geeigneten IT-Sicherheits-Dienstleistern, die über ein reaktiv-/situatives Angebots- und Notfall-Management-Portfolio verfügen.

**Preis:** kostenlos

**Link:** [Anlaufstelle bei IT-Sicherheitsvorfällen](#)

### 🔗 **Hinweisschild Verhalten bei IT-Notfällen**

**Anbieter:** Allianz für Cyber-Sicherheit, Godesberger Allee 185-189, 53175 Bonn, Deutschland

**Beschreibung:** Die IT-Notfallkarte „Verhalten bei IT-Notfällen“ ist ein Hinweisschild, analog zum bekannten Format „Verhalten im Brandfall“. Die aufgeführten Verhaltenshinweisen bei IT-Notfällen aller Art ermöglichen es Organisationen, vom ersten Moment an die richtigen Entscheidungen treffen zu können. Die IT-Notfallkarte wird als PDF-Dokument mit einem editierbaren Textfeld zum Download zur Verfügung gestellt. In das Feld wird die individuelle Rufnummer bei IT-Notfällen eingetragen.

**Preis:** kostenlos

**Link:** [Hinweisschild Verhalten bei IT-Notfällen](#)

### 🔗 **Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel]**

**Anbieter:** Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53175 Bonn, Deutschland

**Beschreibung:** Die Webseite und ihre weiterführenden Unterseiten beschreiben die Problematik von IT-Sicherheitsvorfällen in Unternehmen. Hinweise beziehen sich dabei auf Endsysteme, Server, Anwendungen und die Verarbeitung von Daten mit diesen IT-Systemen sowie auf den richtigen Umgang mit Sicherheitsvorfällen. Ziel ist es, die Kenntnisse wie auch die Aufmerksamkeit von Unternehmen und Mitarbeitenden in diesem Bereich zu erhöhen. Weiterführende Informationen zur Absicherung von IT-Systemen und zu aktuellen Bedrohungen sind ebenfalls verlinkt.

**Preis:** kostenlos

**Link:** [Vorbeugung und Behandlung von Sicherheitsvorfällen](#)

## ▷ **TECH-3: Datensicherung durchführen und testen**

---

### 🔗 **Erklärvideo zum Thema Datensicherung [Video]**

**Anbieter:** Zentrum Digitalisierung.Bayern (ZD.B), Am Tullnaupark 8, 90402 Nürnberg, Deutschland

**Beschreibung:** In diesem zweiminütigen Lehrvideo vom Zentrum Digitalisierung.Bayern wird das Thema Datensicherung verständlich aufbereitet.

**Preis:** kostenlos

**Link:** [Erklärvideo zum Thema Datensicherung](#)

### 🔗 **Grundsätzliches zur Datensicherung [Broschüre/Flyer (Digital)]**

**Anbieter:** Industrie- und Handelskammer für München und Oberbayern, Balanstraße 55-59, 81541 München, Deutschland

**Beschreibung:** Das siebenseitige Merkblatt behandelt thematisch das grundsätzliche Thema Sichern von Daten. Dabei ist in erster Linie der Blick auf die Datensicherung von Endgeräten (PC, Tablet, Mobilgerät) im Fokus, und es wird Grundlagenwissen vermittelt, das hilft, einzuschätzen, welche Optionen es für Datensicherungen gibt.

**Preis:** kostenlos

**Link:** [Grundsätzliches zur Datensicherung](#)

### 🔗 **Was tun bei einem Sicherheitsvorfall? [Artikel]**

**Anbieter:** Mittelstand-Digital Zentrum Chemnitz, Erfenschlager Straße 73, 09125 Chemnitz, Deutschland

**Beschreibung:** Der Artikel beschreibt die Thematik von IT-Sicherheitsvorfällen und was im Umgang mit diesen zu beachten ist. Dabei werden Tipps gegeben für eine Vorbereitung und Absicherung gegen IT-Sicherheitsvorfälle, sowie Hinweise, wie ein Vorfall erkannt werden kann und was im Fall eines Vorfalls zu tun ist um die negativen Auswirkungen zu minimieren.

**Preis:** kostenlos

**Link:** [Was tun bei einem Sicherheitsvorfall?](#)

### 🔗 **Wie sichere ich meine Daten? [Broschüre/Flyer (Print), Broschüre/Flyer (Digital)]**

**Anbieter:** Mittelstand-Digital Zentrum Chemnitz, Erfenschlager Straße 73, 09125 Chemnitz, Deutschland

**Beschreibung:** In dem Informations-Flyer zum Thema Datensicherung werden grundlegende Empfehlungen zur Sensibilisierung und für die Durchführung von Datensicherungen (Backups) gegeben.

**Preis:** kostenlos

**Link:** [Wie sichere ich meine Daten?](#)



## ▷ **TECH-2: Sichere Einstellungen wählen**

---

### 🔗 **Best-Practice-Beispiel: Überraschungsangriff auf die IT [Broschüre/Flyer (Digital)]**

**Anbieter:** Mittelstand 4.0-Kompetenzzentrum Stuttgart, Nobelstraße 12, 70569 Stuttgart, Deutschland

**Beschreibung:** In diesem 2-Seiter des Mittelstand 4.0-Kompetenzzentrums Stuttgart wird anhand eines realen Best-Practice-Beispiels beschrieben, wie Unternehmen vorgehen, wenn sie sich mit einem Verschlüsselungsangriff konfrontiert sehen, sowie welche Maßnahmen getroffen werden können, um nicht erneut Opfer eines Cyberangriffes zu werden.

**Preis:** kostenlos

**Link:** [Überraschungsangriff auf die IT](#)

### 🔗 **Kurz erklärt - 3 Tipps für mehr IT-Sicherheit [Video]**

**Anbieter:** Mittelstand-Digital Zentrum Berlin, Potsdamer Straße 7, 10785 Berlin, Deutschland

**Beschreibung:** In diesem dreiminütigen Video vom Mittelstand 4.0-Kompetenzzentrum Berlin werden drei Tipps für mehr IT-Sicherheit im Unternehmen gegeben.

**Preis:** kostenlos

**Link:** [Kurz erklärt – 3 Tipps für mehr IT-Sicherheit](#)

## ▷ ORG-2: Überblick über die größten Risiken gewinnen

---

### 🔗 CARE-Tool zur Risikoeinschätzung

**Anbieter:** Kriminologisches Forschungsinstitut Niedersachsen e.V., Lützerodestr. 9, 30161 Hannover, Deutschland

**Beschreibung:** CARE bietet Unternehmen eine individuelle Risikoeinschätzung in Bezug auf ihre Gefährdung durch Cyberangriffe. Ergänzend erhalten diese im Anschluss auf die Risiken abgestimmte demographische Informationen, kurze Hintergrundinfos sowie Empfehlungen, was sie an IT-Sicherheitsmaßnahmen mit welcher Priorität angehen sollten.

**Preis:** kostenlos

**Link:** [CARE-Tool zur Risikoeinschätzung](#)

### 🔗 Checkliste IT-Sicherheitsrisiko Mensch [Broschüre/Flyer (Digital)]

**Anbieter:** Mittelstand-Digital Zentrum Berlin, Potsdamer Straße 7, 10785 Berlin, Deutschland

**Beschreibung:** Die zweiseitige Checkliste des Mittelstand 4.0-Kompetenzzentrums Berlin unterstützt KMU in der Beantwortung der Frage, ob ihre Mitarbeiter:innen auf digitale Angriffe vorbereitet und ausreichend zum Thema IT-Sicherheit informiert sind.

**Preis:** kostenlos

**Link:** [Checkliste IT-Sicherheitsrisiko Mensch](#)

### 🔗 DsiN-Sicherheitscheck [Webbasierte IT-Sicherheitsanalyse]

**Anbieter:** Deutschland sicher im Netz e.V., Albrechtstraße 10c, 10117 Berlin, Deutschland

**Beschreibung:** Der DsiN-Sicherheitscheck bietet einen leichten Einstieg zur Ermittlung des IT-Sicherheitsniveaus in kleinen und mittleren Unternehmen (KMU). In wenigen Minuten erhalten Entscheider und Geschäftsführer eine Auswertung mit passenden Handlungsempfehlungen. Neben einer Gesamtauswertung erhalten Sie zudem Auswertungen zu den einzelnen Abschnitten. Die Auswertungstexte bieten Empfehlungen für zu ergreifende Maßnahmen sowie zu weiterführenden Informationen.

**Preis:** kostenlos

**Link:** [DsiN-Sicherheitscheck](#)

### 🔗 Sechs Thesen zur IT-Sicherheit in kleineren und mittleren Unternehmen [Broschüre/Flyer (Digital)]

**Anbieter:** Mittelstand 4.0-Kompetenzzentrum Stuttgart, Nobelstraße 12, 70569 Stuttgart, Deutschland

**Beschreibung:** In diesem Thesenpapier der Arbeitsgruppe IT-Sicherheit von Mittelstand-Digital, unter Federführung des Mittelstand 4.0-Kompetenzzentrum Stuttgart, wurden sechs Thesen zum Thema „IT-Sicherheit in kleineren und mittleren Unternehmen“ entwickelt, welche der Sensibilisierung für das Thema IT-Sicherheit dienen sollen. Das Dokument ist als Impulsgeber für eine vertiefte Diskussion zum Thema gedacht.

**Preis:** kostenlos

**Link:** [Sechs Thesen zur IT-Sicherheit in KMU](#)