Mittelstand-Digital
Zentrum
Handwerk

IT-Sicherheit.

Chancen und Risiken für Handwerksbetriebe.

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

IT-Sicherheit bedeutet Zukunftssicherheit.

Auch im Handwerk werden immer mehr Prozesse digital. Das bedeutet neue Chancen – aber auch Risiken. Denn die Gefahren aus dem Internet sind vielfältig, die Attacken werden raffinierter. Ein IT-Sicherheitskonzept auf neuestem Stand ist also kein Luxus, sondern vielmehr zentrale Voraussetzung für die Digitalisierung des eigenen Betriebs. Die gute Nachricht: Schon mit wenigen Tipps und Tricks sind Sie auf der sicheren Seite.

© HEA

TIPP 1

Schutzmaßnahmen immer kommunizieren.

Für eine IT-Sicherheit, die diesen Namen verdient, kommen verschiedene IT-Sicherheitsprozesse im Unternehmen zum Tragen. Neben rein technischen Lösungen sind dabei auch immer mehr betriebliche Kommunikationsmaßnahmen wichtig. So müssen alle Mitarbeiter regelmäßig informiert werden, wie im Betrieb mit konkreten Situationen umzugehen ist – etwa beim Öffnen von E-Mail-Anhängen, bei der Nutzung von mobilen Endgeräten und der Verwendung von mobilen Datenträgern wie USB-Sticks. Noch wichtiger ist eine Festlegung: Wie sollten sich die Mitarbeiter verhalten, falls der Ernstfall doch einmal eintritt?

TIPP 2

Betriebssysteme regelmäßig updaten.

Stellen Sie bitte sicher, dass nur Betriebssysteme im Einsatz sind, die durch regelmäßige Updates aktuell mögliche Sicherheitslücken immer schnell schließen.
Am sichersten ist die Aktivierung des automatischen Updates – auch wenn dies manchmal etwas Geduld erfordert.

TIPP 3

Nur wenige Geräte mit dem Internet verbinden.

Eine einfache Lösung, sich vor Gefahren zu schützen, ist, wenn es im Betrieb nur einen PC gibt, der mit dem Internet verbunden ist. Hier kommt natürlich nur ein System in Frage, das keine wichtigen Betriebsdaten enthält. Die Methode kann noch optimiert werden, wenn ein Betriebssystem auf Linux-Basis oder macOS genutzt wird, das von vielen Schadprogrammen nicht betroffen ist.

TIPP 4

Mobilgeräte besonders gut absichern.

Bei mobilen Endgeräten gilt ebenfalls immer die Update-Regel. Bereits die Auswahl des Betriebssystems sollte unter Sicherheitsaspekten erfolgen – bei Android-Geräten sind meist umfangreichere Sicherheitsmaßnamen erforderlich. Mobile Endgeräte sind in verschiedensten Netzen unterwegs und damit stärker gefährdet als der PC im Betrieb. Daher sollten einige Grundregeln befolgt werden:

- Verschlüsselung der gespeicherten Daten einrichten
- Funkschnittstellen (WLAN und Bluetooth) nur dann aktivieren, wenn sie wirklich gebraucht werden
- Möglichst keine wichtigen Firmendaten auf Smartphones oder Tablets ablegen
- Für den Zugriff auf sensible Firmendaten ausschließlich VPN-Lösungen nutzen – unabhängig davon, ob die Daten auf dem Betriebsserver oder in der Cloud liegen

Es geht um die Existenz Ihres Betriebs.

Leider nimmt die Zahl der Bedrohungen durch sogenannte Schadware, also Programme, die Schäden an den IT-Systemen verursachen, dramatisch zu. Trotzdem haben immer noch erschreckend wenige Handwerksbetriebe, vor allem kleinere, entsprechende IT-Sicherheitsmaßnamen ergriffen. Wer mit digitalen Geräten arbeitet, sollte aber wissen, welche Gefahren lauern, was Attacken anrichten können – und wie man ihnen erfolgreich begegnet.

Kleine Unternehmen werden oft attackiert.

Immer mehr Betriebe werden Ziel von Cyber-Attacken, die zu einem kompletten Datenverlust führen können – vor allem dann, wenn keine Datensicherung durchgeführt wird. Viele Handwerker denken noch, ihr Betrieb sei viel zu klein, um das Interesse der Hacker auf sich zu ziehen. Ein großer Irrtum! Denn oft versuchen Hacker gezielt, über kleine Betriebe an große Unternehmen heranzukommen. Andere Bedrohungen haben gar kein konkretes Ziel und können trotzdem verheerenden Schaden anrichten. Verschlüsselungstrojaner, die PC-Daten in »Geiselhaft« nehmen, sind ein besonders drastisches Beispiel aus der letzten Zeit.

5 Kategorien für Gefahren:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Welche Bedrohungen gibt es überhaupt?

Schadware sind Programme, die meist unbemerkt im Hintergrund laufen oder erst dann bemerkt werden, wenn es schon zu spät ist. Diese Programme finden ihren Weg auf PC und mobile Endgeräte auf unterschiedliche Weise, um sofort oder später aktiv zu werden. Hier eine Übersicht über die häufigsten Bedrohungen, die in Form von Schadprogrammen wirksam werden können – meist durch menschliche Fehler:

Viren
Sie nisten sich in Nutzdateien ein und benötigen wie biologische Viren einen Wirt. Viren verändern Programme und Daten so, dass sie nicht mehr genutzt werden können, weiteren Schaden anrichten oder den Computer erheblich verlangsamen. Sie verbreiten sich zwar auf dem Computer, aber nicht im Netz.

Trojaner
Trojaner, Spyware und Backdoors sind Programme, die so aussehen, wie eine häufig verwendete Anwendung – beispielsweise explorer.exe. Neben der eigentlichen Aufgabe übernehmen sie aber unerwünschte Funktionen. Trojaner sind oft in E-Mail-Anhängen, PDF-Dateien und Spiele-Dateien versteckt, aktivieren sich bei Doppelklick und verbreiten sich wie Würmer oft selbsttätig weiter. Einige geben Passwörter an den Angreifer weiter bzw. ermöglichen einen vollständigen Einblick in oder sogar den Zugriff auf den attackierten Computer.

Würmer
Als eigenständige Programme benötigen Würmer keinen Wirt, sondern verbreiten sich selbsttätig über das Netz. Sie nutzen oft Lücken im Betriebssystem aus und führen zu einer verlangsamten Arbeitsweise des Computers, weil sie dem Prozessor Leistung und Speicher entziehen.

Exploits
Exploits führen DoS-Angriffe durch, die den Internetzugang, das Betriebssystem oder die Dienste eines Hosts belasten. Oder sie versuchen, unautorisiert Zugriffsrechte auf Unternehmensdaten zu erlangen. In vielen Fällen ist die Zerstörung des Betriebssystems das eigentliche Ziel der Exploits.

Rootkits
Hinter diesem Begriff verbirgt sich Schadware, die sich besonders tief im Betriebssystem versteckt und für Virenscanner nur schwer zu finden ist. Linux- und Windows-Systeme sind gefährdet. Rootkits schädigen auf ähnliche Weise wie Trojaner.

Wenn solche Schadprogramme ins Unternehmen gelangen, steht möglicherweise die Existenz auf dem Spiel. Deshalb sollten sich auch kleinere Betriebe unbedingt schützen und Attacken sehr ernst nehmen. Eine Animation, die zeigt, wie Schadware auf lokale Rechner gelangt, finden Sie hier:

Der beste Weg zur sicheren Lösung.

Die Vorteile guter IT-Sicherheit liegen auf der Hand. Weil die erforderlichen Investitionen aber nicht direkt mit einer Umsatzsteigerung verbunden sind, wird das Thema oft auf später verschoben. Lassen Sie einen Sicherheits-Check von einem Experten durchführen. So kommen Sie am schnellsten und bequemsten zu einer Sicherheitslösung, auf die Verlass ist.

Einbrecher kommen nicht nur durchs Fenster.

Jeder Unternehmer muss für sich selbst feststellen, welche Folgen ein Ausfall der IT-Systeme für ihn bedeuten kann. Viele Handwerker können aber nicht selbst einschätzen, auf welchem Niveau sich ihre Sicherheitsmaßnahmen bewegen. Denn während Einbrecher früher durchs Fenster kamen, gehen Cyber-Kriminelle heute deutlich raffinierter vor. Oft bemerkt man eine Attacke erst, wenn es zu spät ist. Mit der zunehmenden Digitalisierung auch von Werkzeugen und Maschinen kann ein Betrieb im schlimmsten Fall sogar komplett stillgelegt werden. Moderne IT-Sicherheitslösungen und -prozesse schützen vor solchen Katastrophen.

IT-Sicherheit muss gelebt werden!

Wer sich mit Digitalisierung, in welcher Art und Weise auch immer befasst, muss sich zwangsläufig mit dem Thema IT-Sicherheit auseinandersetzen. Inzwischen gibt es zwar immer mehr technische Sicherheitsmaßnahmen in den Betrieben, diese sind aber oft nur bedingt wirksam, denn es reicht nicht aus, das Gewissen durch technische Lösungen zu beruhigen. IT-Sicherheit muss gelebt werden – und sie ist Chefsache!

Guter Schutz braucht Expertise.

Ein unabhängiger Spezialist kann beispielsweise anhand von Checklisten ein konkretes Bild zum Ist- und Soll-Zustand der IT-Sicherheit erstellen. Aus diesen Ergebnissen lässt sich ein gezielter Optimierungsplan erstellen. Eine Zertifizierung, die direkt aus dem Handwerk heraus speziell für das Handwerk entwickelt wurde, ist der E-CHECK IT des ZVEH. Weiterhin gibt es nützliche Tools wie den Routenplaner „Cyber-Sicherheit für Handwerksbetriebe“, der gemeinsam von KDH und BSI entwickelt wurden. Dieser stellt eine Schritt-für-Schritt-Anleitung dar, wie Unternehmer ihren Betrieb sicherer machen können.

Eine Geschäftschance für IT-Fachbetriebe.

Fachbetriebe im IT-Handwerk können sich in diesem Themenfeld ein attraktives neues Geschäftsfeld erschließen. Dazu müssen sie sich natürlich zunächst das entsprechende Know-how für die Werkzeuge aneignen, mit denen ein IT-Check für Handwerksbetriebe durchgeführt werden kann.

Empfohlene Tools.

Der Routenplaner für Cyber-Sicherheit im Handwerk:

Informationen zum Routenplaner für Cyber-Sicherheit:

E-CHECK IT:

Checkliste für IT-Sicherheit im Handwerksbetrieb:

Das Mittelstand-Digital Zentrum Handwerk.

Mit über einer Million Betrieben ist das Handwerk zentraler Teil der deutschen Wirtschaft. Das Zentrum bietet Expertenwissen, Demonstrationszentren, Best-Practice-Beispiele sowie Netzwerke zum Erfahrungsaustausch.

Wir helfen bei der Digitalisierung.

Das Mittelstand-Digital Zentrum Handwerk bietet für jeden Handwerksbetrieb praktische Informations-, Qualifikations- und Unterstützungsangebote:

- Broschüren, Checklisten, Online-Ratgeber
- Demonstration digitaler Anwendungen
- Workshops und Fachveranstaltungen
- Webinare und Präsenzschulungen
- Entwicklung von praxisnahen Implementierungsstrategien
- Betriebsübergreifender Erfahrungsaustausch Begleitung bei der Umsetzung von digitalen Projekten

Das Zentrum stellt sein Expertenwissen in einem kostenfreien und anbieterneutralen Angebot deutschlandweit zur Verfügung. Es führt Schulungen durch, informiert und sensibilisiert die Betriebe bezüglich der Einsatzmöglichkeiten digitaler Technologien und gibt Hilfestellungen zur praktischen Umsetzung. Informationen über das gesamte Angebot finden Handwerksbetriebe auf: **www.handwerkdigital.de**

Eine Förderinitiative des BMWi.

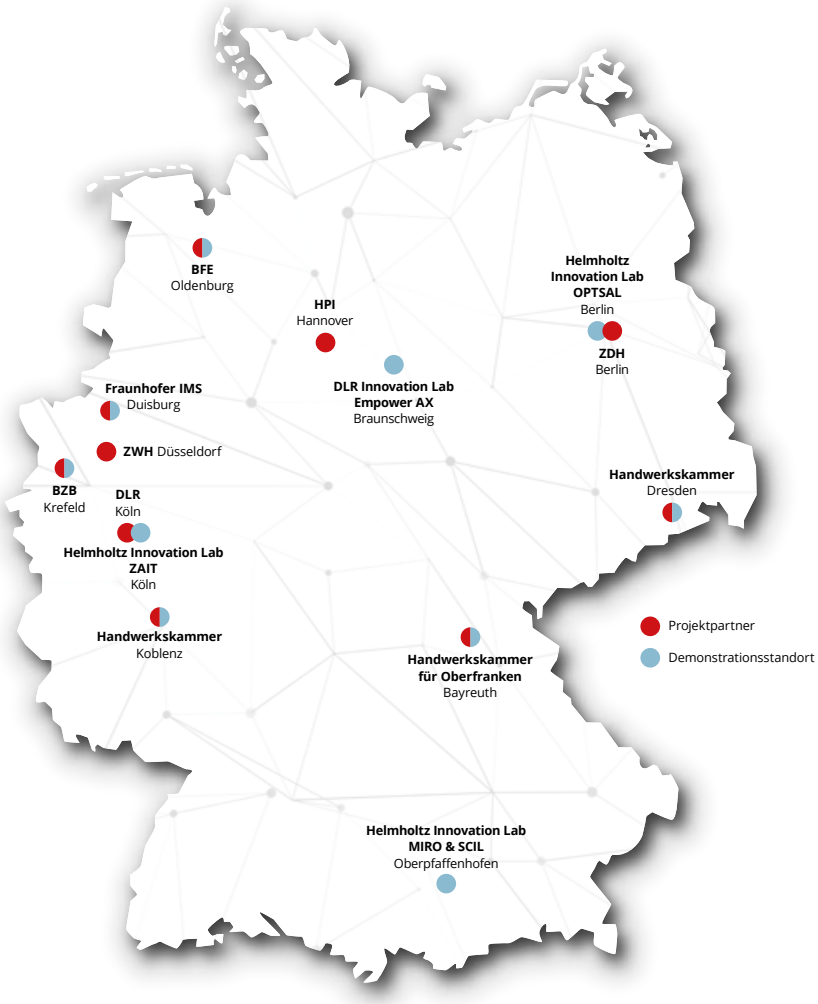
Das Mittelstand-Digital Zentrum Handwerk gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Zentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter: **www.mittelstand-digital.de**

Kostenfreie und anbieterneutrale Angebote

Mittelstand-Digital
Zentrum Handwerk

Wo Sie auch sind, wir sind ganz in der Nähe.



Impressum.

Herausgeber
Mittelstand-Digital Zentrum Handwerk
Schaufenster Informations- und Kommunikationstechnologien
Bundestechnologiezentrum für Elektro- und Informationstechnik e. V. (BFE)
Donnerschweer Straße 184
26123 Oldenburg

Autor
Dipl.-Ing. Rainer Holtz (BFE)

Zentralverband des Deutschen Handwerks e. V. (ZDH)
Mohrenstraße 20/21
10117 Berlin

Redaktion
Stephan Blank (ZDH),
Juliane Haase (ZDH)

Gestaltung
MÜLLER MÖLLER BRUSS

Folgen Sie uns:

handwerkdigital.de
handwerkdigital
HaWe_Digital
Mittelstand-Digital Zentrum Handwerk
digitales_handwerk

Stand: 06/2022

Hinweis:
Für eine bessere Lesbarkeit wird in diesem Medium das generische Maskulinum für Wörter wie Teilnehmer, Mitarbeiter, Unternehmer etc. verwendet. Selbstverständlich sind immer Menschen aller Geschlechtsidentitäten gemeint.