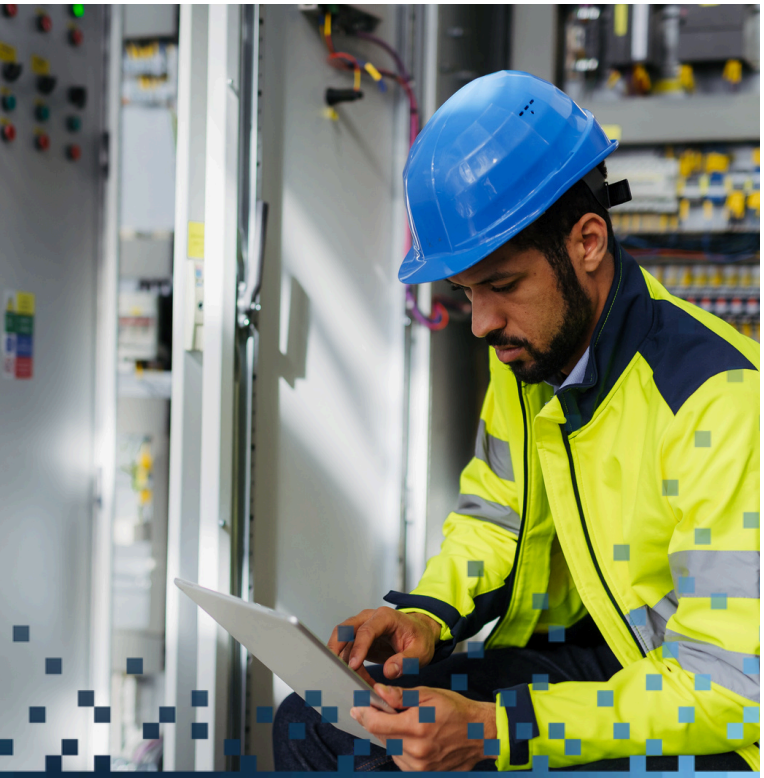
CYBERsicher OT-CRAft Sichere Geräte. Resiliente Anlagen.



Security-Basics für Anlagenbetreiber

Eine Lernplattform für Kleine und Mittlere Unternehmen (KMU) für mehr Resilienz in kritischen Infrastrukturen.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Kurs Security-Basics

Security-Basics steht Ihnen kostenfrei auf ot-craft.de zur Verfügung. In einer Spielsituation lernen Sie, welche Rolle Cybersicherheit für die Betriebssicherheit hat, und testen Ihr Wissen direkt in kurzen Quizfragen. Der Kurs Security-Basics behandelt die Themen:

- Grundlagen der Cybersicherheit, z. B. Bedrohungen und Angreifertypen
- Ransomware: Ablauf, Risiken und wirksame Schutzmaßnahmen
- Vorbereitung auf den Ernstfall: Notfallpläne und Netzwerksegmentierung

Noch mehr von OT-CRAft entdecken

OT-CRAft wendet sich an Hersteller und Integratoren sowie Anlagenbetreiber. Lernen Sie alle Angebote kennen, kostenfrei und herstellerneutral unter ot-craft.de.

Folgen Sie uns auf **LinkedIn**

1x im Quartal den **Newsletter** erhalten

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Über OT-CRAft
OT-CRAft gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und im Handwerk. OT-CRAft ist eine Kooperation von THA_innos und DZ.S.

THA Technische Hochschule Augsburg | THA_innos Institut für innovative Sicherheit

DZ.S Digitales Zentrum Schwaben

Impressum

Herausgeber:
Digitales Zentrum Schwaben (DZ.S) IT-Gründerzentrum GmbH
Werner-von-Siemens-Str. 6
D-86159 Augsburg
info@cyber-resilience-kmu.de
www.ot-craft.de

Redaktion:
Digitales Zentrum Schwaben
Sabrina Harper
info@cyber-resilience-kmu.de

Gestaltung und Produktion:
Digitales Zentrum Schwaben

Bildnachweis:
Canva Pro (Titel)

Druck:
Online-Version

Stand:
August 2026

Wissen schützt den Betriebsablauf

Ein Cyberangriff muss nicht spektakulär beginnen. Ein unsicheres Passwort oder eine offene Fernwartungsverbindung genügt, und schon könnte die Produktion stillstehen. Für Betreiber*innen kritischer Infrastrukturen ist Cybersicherheit deshalb Teil der Betriebssicherheit, nicht nur ein IT-Thema.

Drei Schutzziele zeigen, was dabei auf dem Spiel steht: Vertraulichkeit, Integrität und Verfügbarkeit, zusammen auch als CIA bekannt. Sie helfen einzuordnen, ob Daten unbefugt eingesehen, unbemerkt verändert oder im Ernstfall nicht mehr verfügbar sein könnten.

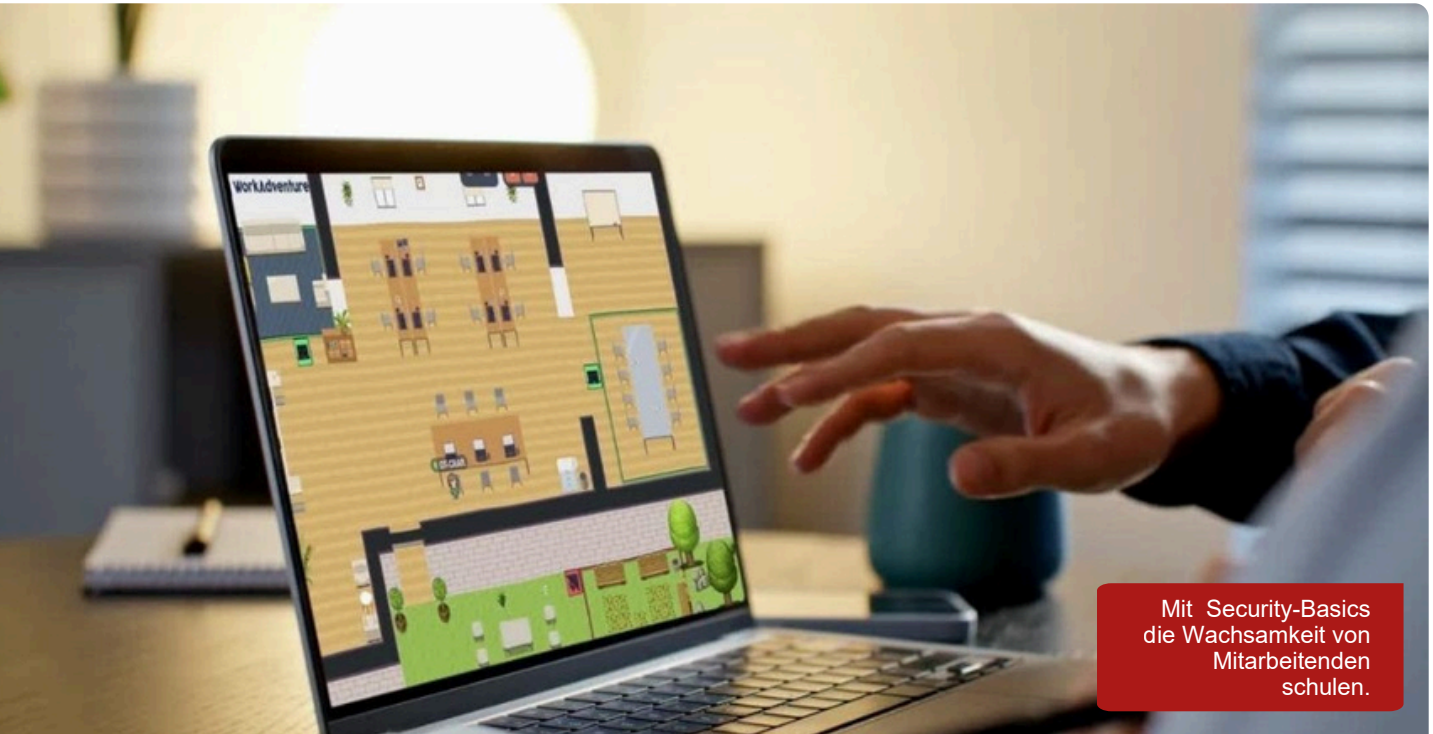
Security-Basics vermittelt wichtiges Grundwissen: verständlich, praxisnah und ohne Vorkenntnisse. In einem simulierten Unternehmen bearbeiten Sie an virtuellen Arbeitsplätzen kompakte Lerninhalte und beantworten anschließend Quizfragen zu den zentralen Themen der Cybersicherheit.

Wie Angriffe ablaufen

Häufig genügt eine Phishing-E-Mail, die täuschend echt aussieht und zur Herausgabe sensibler Daten verleitet, oder eine Firewall, die aus Versehen offen im Internet erreichbar ist. Auch bekannte Sicherheitslücken in veralteter Software werden automatisiert ausgenutzt, oft ohne dass jemand gezielt danach sucht.

Ist ein Angreifer erst einmal im Netz, bleibt er selten dort, wo er eingedrungen ist: Über weitere Schwachstellen bewegt er sich unerkannt weiter. Das kann etwa vom IT- ins OT-Netz sein, also vom Büro rein in die Produktionsanlagen. Dies bezeichnet man als Lateral Movement, zu Deutsch Seitwärtsbewegung. Dafür eignen sich insbesondere Dienstleister mit privilegierten Zugängen, sie zählen zu den attraktivsten Zielen.

Security-Basics zeigt auf, wie Angriffswege im eigenen Betrieb aussehen können und schult so die Wachsamkeit von Mitarbeitenden im Betrieb.



Mit Security-Basics die Wachsamkeit von Mitarbeitenden schulen.

Wer Unternehmen angreift

Wie gezielt ein Angriff erfolgt, hängt stark vom Angreifenden ab:

Staatliche Akteur*innen verfügen über sehr hohe Ressourcen und nehmen gezielt kritische Unternehmen oder Infrastrukturen ins Visier.

Die **organisierte Kriminalität** wirft mit hohen Ressourcen ein breiteres Netz über Unternehmen aller Größenordnungen.

Rivalisierende Einzelpersonen oder Gruppen sowie unbeabsichtigt Handelnde ohne Schadensziel ergänzen die Bedrohungslage.

Der richtige Schutz

Eine hundertprozentige Absicherung ist weder möglich noch wirtschaftlich sinnvoll. Entscheidend ist die richtige Kombination aus Maßnahmen: Sie reduzieren Angriffsmöglichkeiten und erhalten die Handlungsfähigkeit im Ernstfall.

Eine strukturierte Risikoanalyse hilft zum Beispiel dabei, die passenden Maßnahmen für den eigenen Betrieb zu finden.

Und essenziell ist das Wissen der Angestellten. Durch Awareness-Maßnahmen wie die Inhalte auf der Lernplattform können Produktionsmitarbeitende, IT-Leiter*innen, Fabrikangestellte und viele weitere Berufsgruppen schneller einschätzen, wo Gefahrenstellen lauern und dementsprechend handeln.

80% von 950 Ransomware-Angriffen in Deutschland trafen KMU.

BSI-Lagebericht 2025