CYBERsicher

ReACD
Reaktion trainieren,
im Ernstfall sicher.

IT-Sicherheit
IN DER WIRTSCHAFT

ReACD

Reaktion auf Cybersicherheitsvorfälle und Datenverlust

Technology
Arts Sciences
TH Köln

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital

Haben Sie schon mal eine Phishing-Mail erhalten?

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Haben Sie schon mal auf eine Phishing-Mail geklickt?

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Bundeslagebild Cybercrime 2024

- **131.391 Cybercrime-Fälle:** finanzstarke als auch KMUs betroffen
- **950 Ransomware-Delikte:** tägliche Zunahme um 2-3 neue Angriffe
- **Finanzieller Schaden:** 178,6 Milliarden €
- **Vergleich zum Vorjahr:** Anstieg um 30 Milliarden €

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Warum wächst Cyberkriminalität?

- **Technologie**: Künstliche Intelligenz kann automatisierte Angriffe begünstigen
- **Lukratives Geschäftsmodell:**
  - zunehmende Organisation in kriminellen Vereinigungen
  - Cyberkriminalität als Geschäftsmodell mit hohem Umsatzpotential
- **Gesellschaft:** Alltag ist digitalisiert und viele Nutzer sind nicht sensibilisiert

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

IT-Sicherheitsschulungen (Auszug)

- BSI IT-Grundschutz-Schulungen
- Sichere Softwareentwicklung
- Sichere Passwörter
- Multifaktor-Authentifizierung
- Phishing-Training

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Verbesserung von nur 1,7 Prozent: Phishing-Training fast immer wirkungslos

Eine große Studie in einem US-Gesundheitsunternehmen zeigt, dass gängige Phishing-Trainings das Risiko kaum senken – egal wie intensiv oder interaktiv sie sind.

333

(Bild: iX)

18.08.2025, 10:06 Uhr Lesezeit: 3 Min. | iX Magazin

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Fazit zur verschärften Bedrohungslage

- IT-Sicherheitsschulungen haben nur begrenzten Effekt und werden eher als Last gesehen
- Angriffsarten werden raffinierter, ausgeklügelter und automatisiert(er)
- Es ist nur eine Frage der Zeit, bis ein IT-Sicherheitsvorfall auftritt

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

ReACD

Reaktion auf Cybersicherheitsvorfälle und Datenverlust

- Öffentlich gefördertes Projekt
- **Laufzeit:** 1. November 2024 bis 31. Oktober 2027
- **Projektförderer:** Bundesministerium für Wirtschaft und Energie (BMWE)
- **Projektträger:** Deutsches Zentrum für Luft- und Raumfahrt (DLR)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

ReACD-Projektziele

- Fokus auf **KMUs, Startups** und **Handwerksbetriebe**
- Die Handlungsfähigkeit bei IT-Notfällen zu optimieren
- Projektbestandteile
  - Multiplayer Serious Game
  - Conversational Artificial Intelligence
  - Schulungskonzept

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Projektverantwortliche


Paul Varney


Leonard Grabow


Furkan Sengül


Prof. Dr. Valérie Varney


Prof. Dr. Anja Richert


Prof. Dr. Hoai Viet Nguyen


Dr. Eva-Maria Grommes

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Multiplayer Serious Game (MSG)

- Modulares Rollenspiel zum Training der Reaktion auf Cybersicherheitsvorfälle
- Simulation verschiedener realitätsbezogener Cyberangriffe wie z.B.
  - Phishing
  - Social Engineering
  - Ransomware
  - Malware
- Online Multiplayer-Modus spielbar auf Projektwebseite

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Conversational Artificial Intelligence (CAI)

- KI-Chatbot zur Beantwortung von Cybersicherheitsfragen
- CAI verwendbar über die Projektwebseite
- Integration der CAI im Spiel als weitere Unterstützung

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Schulungskonzept

- Vermittlung von Wissen zum korrekten Verhalten bei Cybersicherheitsvorfällen
- Durchspielen/Simulation von Cybersicherheitsvorfällen basierend auf MSG
- Schwachstellen im Notfallmanagement identifizieren
- Optimierungspotentiale bei Notfällen erkennen
- Ermittlung von neuen Use Cases und Verbesserungen bestehender im MSG

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Demo

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Was kann ich jetzt tun

- Frühzeitig bzw. in Friedenszeiten aktiv werden
- Mit IT-Sicherheitsdienstleistern in Kontakt treten und Vorbereitungen treffen
- Notfallpläne erstellen
- Cybersicherheitsvorfälle regelmäßig durchspielen
- Angebote der Transferstelle Cybersicherheit und BSI wahrnehmen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

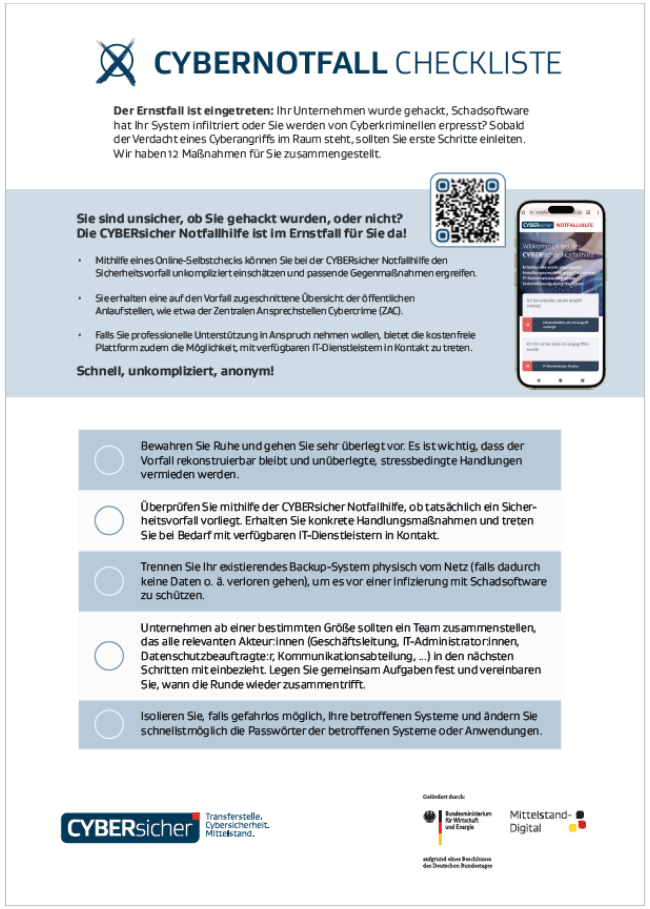
https://transferstelle-cybersicherheit.de/cyberdialog/

https://transferstelle-cybersicherheit.de/cybersicher-check/

https://transferstelle-cybersicherheit.de/notfall/

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital



CYBERNOTFALL CHECKLISTE

Der Ernstfall ist eingetreten: Ihr Unternehmen wurde gehackt, Schadsoftware hat Ihr System infiltriert oder Sie werden von Cyberkriminellen erpresst? Sobald der Verdacht eines Cyberangriffs im Raum steht, sollten Sie erste Schritte einleiten. Wir haben 12 Maßnahmen für Sie zusammengestellt.

Sie sind unsicher, ob Sie gehackt wurden, oder nicht? Die CYBERsicher Notfallhilfe ist im Ernstfall für Sie da!

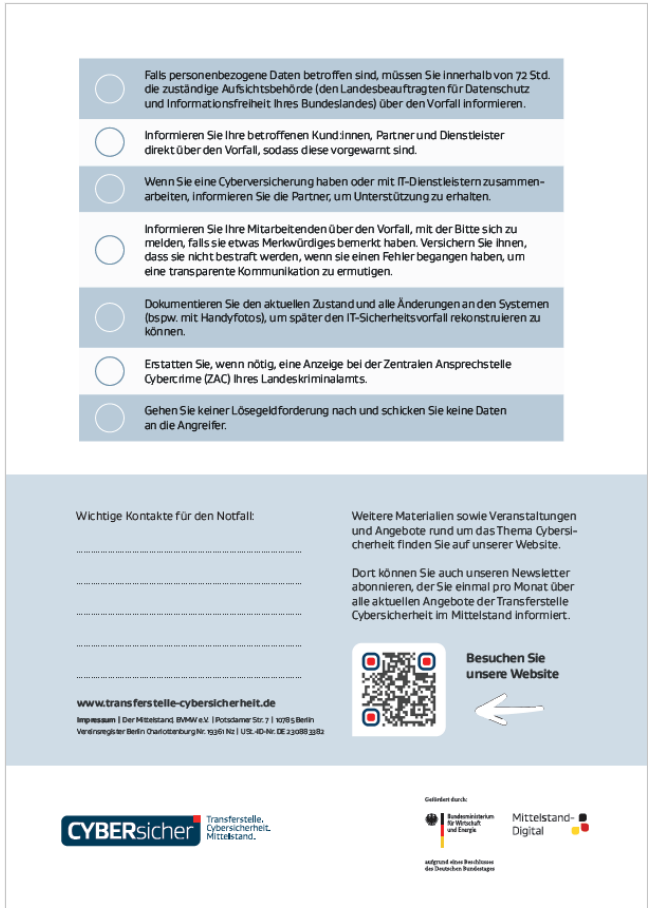
- Mithilfe eines Online-Selbstchecks können Sie bei der CYBERsicher Notfallhilfe den Sicherheitsvorfall unkompliziert einschätzen und passende Gegenmaßnahmen ergreifen.
- Sie erhalten eine auf den Vorfall zugeschnittene Übersicht der öffentlichen Anlaufstellen, wie etwa der Zentralen Ansprechstellen Cybercrime (ZAC).
- Falls Sie professionelle Unterstützung in Anspruch nehmen wollen, bietet die kostenfreie Plattform zudem die Möglichkeit, mit verfügbaren IT-Dienstleistern in Kontakt zu treten.

Schnell, unkompliziert, anonym!

- Bewahren Sie Ruhe und gehen Sie sehr überlegt vor. Es ist wichtig, dass der Vorfall rekonstruierbar bleibt und unüberlegte, stressbedingte Handlungen vermieden werden.
- Überprüfen Sie mithilfe der CYBERsicher Notfallhilfe, ob tatsächlich ein Sicherheitsvorfall vorliegt. Erhalten Sie konkrete Handlungsmaßnahmen und treten Sie bei Bedarf mit verfügbaren IT-Dienstleistern in Kontakt.
- Trennen Sie Ihr existierendes Backup-System physisch vom Netz (falls dadurch keine Daten o. ä. verloren gehen), um es vor einer Infizierung mit Schadsoftware zu schützen.
- Unternehmen ab einer bestimmten Größe sollten ein Team zusammenstellen, das alle relevanten Akteur:innen (Geschäftsleitung, IT-Administrator:innen, Datenschutzbeauftragte:r, Kommunikationsabteilung, ...) in den nächsten Schritten mit einbezieht. Legen Sie gemeinsam Aufgaben fest und vereinbaren Sie, wann die Runde wieder zusammentrifft.
- Isolieren Sie, falls gefahrlos möglich, Ihre betroffenen Systeme und ändern Sie schnellstmöglich die Passwörter der betroffenen Systeme oder Anwendungen.

CYBERsicher Transferstelle Cybersicherheit Mittelstand.

Gefördert durch: Bundesministerium für Wirtschaft und Energie, Mittelstand-Digital, aufgrund eines Beschlusses des Deutschen Bundestages



- Falls personenbezogene Daten betroffen sind, müssen Sie innerhalb von 72 Std. die zuständige Aufsichtsbehörde (den Landesbeauftragten für Datenschutz und Informationsfreiheit Ihres Bundeslandes) über den Vorfall informieren.
- Informieren Sie Ihre betroffenen Kund:innen, Partner und Dienstleister direkt über den Vorfall, sodass diese vorgewarnt sind.
- Wenn Sie eine Cyberversicherung haben oder mit IT-Dienstleistern zusammenarbeiten, informieren Sie die Partner, um Unterstützung zu erhalten.
- Informieren Sie Ihre Mitarbeitenden über den Vorfall, mit der Bitte sich zu melden, falls sie etwas Merkwürdiges bemerkt haben. Versichern Sie ihnen, dass sie nicht bestraft werden, wenn sie einen Fehler begangen haben, um eine transparente Kommunikation zu ermutigen.
- Dokumentieren Sie den aktuellen Zustand und alle Änderungen an den Systemen (bspw. mit Handyfotos), um später den IT-Sicherheitsvorfall rekonstruieren zu können.
- Erstatten Sie, wenn nötig, eine Anzeige bei der Zentralen Ansprechstelle Cybercrime (ZAC) Ihres Landeskriminalamts.
- Gehen Sie keiner Lösegeldforderung nach und schicken Sie keine Daten an die Angreifer.

Wichtige Kontakte für den Notfall:

.....

.....

.....

.....

.....

www.transferstelle-cybersicherheit.de

Impressum | Der Mittelstand. BVMW e.V. | Potsdamer Str. 7 | 10785 Berlin
Vereinsregister Berlin Charlottenburg Nr. 9361 Nz | USt-ID-Nr. DE 230883382

Weitere Materialien sowie Veranstaltungen und Angebote rund um das Thema Cybersicherheit finden Sie auf unserer Website.

Dort können Sie auch unseren Newsletter abonnieren, der Sie einmal pro Monat über alle aktuellen Angebote der Transferstelle Cybersicherheit im Mittelstand informiert.

Besuchen Sie unsere Website

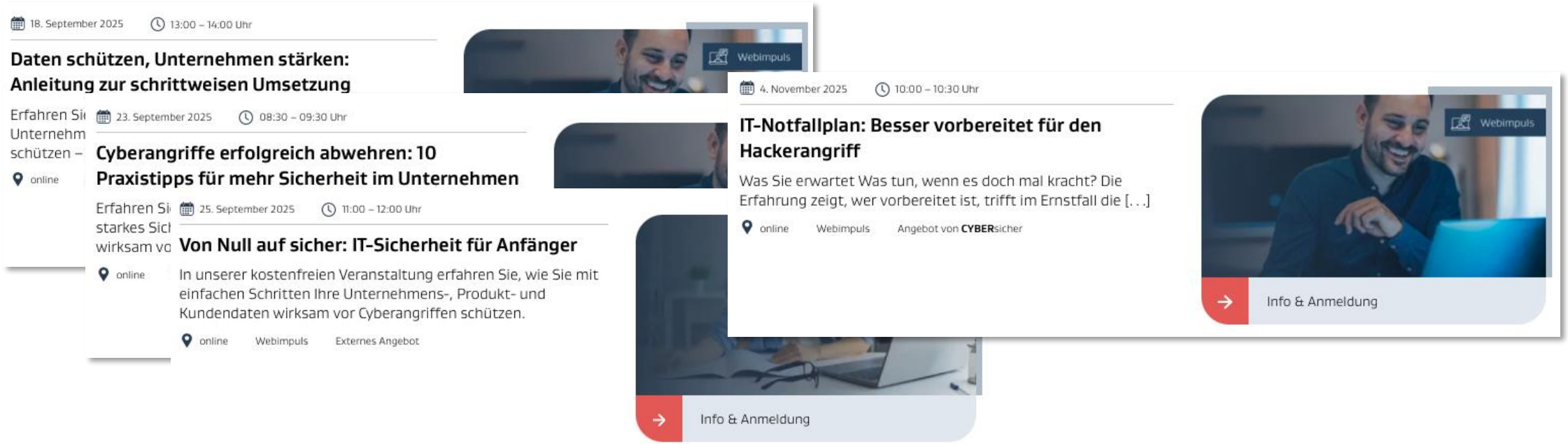
CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

Gefördert durch: Bundesministerium für Wirtschaft und Energie, Mittelstand-Digital, aufgrund eines Beschlusses des Deutschen Bundestages

https://transferstelle-cybersicherheit.de/material/die-cybernotfall-checkliste/

Gefördert durch: Bundesministerium für Wirtschaft und Energie, Mittelstand-Digital, aufgrund eines Beschlusses des Deutschen Bundestages

Weitere Angebote & IT-Notfallplan



https://transferstelle-cybersicherheit.de/veranstaltungen/

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitsdienstleister

- Bewertung der Kompetenz des Dienstleisters
- Dienstleister soll bei Erstellung von Notfallplan unterstützen
- Eventuell externe SOC-Dienstleistung wahrnehmen

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-OrganisationenCyberRisikoCheck/Informationen-und-Empfehlungen/KMU//SucheDienstleister/suche_node.html

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Wir benötigen Sie

- Als Partner um das Schulungskonzept durchzuführen und zu erproben
- Interviews für
  - Erfassung von Use Cases
  - Identifizierung von positiven und negativen Maßnahmen
- Feedback zum MSG
- Sprechen Sie mit uns

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Fazit

Es wird passieren!

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Weitere Informationen

- Projektwebseite: https://reacd.de
- Folien: https://reacd.de/slides
- MSG bald spielbar über die Projektwebseite

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Abschlussfragen

War Ihr Unternehmen schon mal Opfer eines Cyberangriffs?

Was waren Ihre negativen Reaktionsmaßnahmen?

Was waren Ihre positiven Reaktionsmaßnahmen?

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

CYBERsicher ReACD Reaktion trainieren, im Ernstfall sicher.

IT-Sicherheit IN DER WIRTSCHAFT

VIELEN DANK

für Ihre Aufmerksamkeit!

Technology Arts Sciences TH Köln

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital