

ReACD

Reaktion auf Cybersicherheitsvorfälle und Datenverlust

**Haben Sie schon mal
eine Phishing-Mail
erhalten?**

**Haben Sie schon mal
auf eine Phishing-Mail
geklickt?**

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 €

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

IT-Sicherheitsschulungen (Auszug)

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

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

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

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)

ReACD-Projektziele

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

Projektverantwortliche



Paul Varney



Leonard Grabow



Furkan Sengül



Prof. Dr. Valérie Varney



Prof. Dr. Anja Richert



Prof. Dr. Hoai Viet Nguyen



Dr. Eva-Maria Grommes

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

Conversational Artificial Intelligence (CAI)

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

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

Demo



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

Die CYBERDialoge

Cybersicherheit in meinem Betrieb – wo soll ich da anfangen? Das klären wir persönlich und gemeinsam in unserem Erstgespräch, dem **CYBERDialog**.

Erfahren Sie in unserem praktischen Onlineformat innerhalb einer Stunde, wie Sie am besten in das Thema Cybersicherheit einsteigen. Dabei werden Gefahrenquellen identifiziert und erste Maßnahmen besprochen, sodass Sie direkt loslegen können, die Cybersicherheit in Ihrem Unternehmen zu erhöhen!



Jetzt **CYBERDialog** buchen

Sie sind nur noch einen Schritt davon entfernt, die Cybersicherheit in Ihrem Unternehmen dauerhaft zu verbessern.

Wählen Sie einen freien Slot über die Buchungsseite und sprechen Sie direkt mit einem unserer Experten!

→ Zur Buchung

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

CYBERSicher Check

Mit dem **CYBERSicher Check** jetzt **schnell und einfach** die IT-Sicherheit in Ihrem Unternehmen anpacken!

Ermitteln Sie mit unserem praktischen Tool den Ist-Zustand Ihrer IT-Sicherheit und erhalten Sie individuell auf Ihr Unternehmen zugeschnittene Handlungsempfehlungen sowie passende Materialien aus unserer Datenbank.

Die Nutzung ist dabei so einfach wie möglich gehalten. Beantworten Sie einfach die Fragen aus den Teilbereichen Datenschutz, Datensicherung, Informationssicherheit, IT-Systeme, Schulungen und Verantwortlichkeiten und der **CYBERSicher Check** ermittelt Ihre ganz **persönlichen Verbesserungspotenziale** automatisch!



Jetzt die IT-Sicherheit im Unternehmen anpacken

Ganz einfach den Zustand Ihrer IT-Sicherheit ermitteln, Handlungsempfehlungen erhalten und passende Materialien nutzen. Ein echter Mehrwert für Ihr Unternehmen!

→ Zum CYBERSicher Check

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

Notfall – Ein Cybersicherheitsangriff

Sie vermuten einen Angriff oder werden sogar erpresst? Erhalten Sie mit der **CYBERSicher Notfallhilfe** innerhalb von wenigen Minuten Unterstützung durch praxisorientierte Tipps oder den Kontakt zu IT-Dienstleistern.



CYBERSicher Notfallhilfe

Sie glauben, ein Cyberangriff liegt vor? Dann erhalten Sie hier mit wenigen Klicks Hilfe.

Hier bekommen Sie nicht nur Gewissheit, ob ein Cyberangriff vorliegt, sondern auch direkt Empfehlungen, wie Sie reagieren können.

→ Zur CYBERSicher Notfallhilfe

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

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 Akteure (Geschäftsleitung, IT-Administratorinnen, Datenschutzbeauftragte, 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.
- ☐ Erstellen 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:

.....
.....
.....
.....
.....

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**

www.transferstelle-cybersicherheit.de
Impressum | Der Mittelstand, BfM e.V. | Potsdamer Str. 7 | 10115 Berlin
Vereinsregister Berlin (Handelsregister Nr. 15316 N) | USt-Id-Nr. DE 23088 3382

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/>

Weitere Angebote & IT-Notfallplan

18. September 2025 13:00 – 14:00 Uhr

**Daten schützen, Unternehmen stärken:
Anleitung zur schrittweisen Umsetzung**

Erfahren Sie, wie Sie Ihr Unternehmen schützen –

online

23. September 2025 08:30 – 09:30 Uhr

**Cyberangriffe erfolgreich abwehren: 10
Praxistipps für mehr Sicherheit im Unternehmen**

Erfahren Sie, wie Sie Ihr Unternehmen wirksam vor Cyberangriffen schützen.

online Webimpuls Externes Angebot

25. September 2025 11:00 – 12:00 Uhr

Von Null auf sicher: IT-Sicherheit für Anfänger

In unserer kostenfreien Veranstaltung erfahren Sie, wie Sie mit einfachen Schritten Ihre Unternehmens-, Produkt- und Kundendaten wirksam vor Cyberangriffen schützen.

online Webimpuls Externes Angebot

4. November 2025 10:00 – 10:30 Uhr

IT-Notfallplan: Besser vorbereitet für den Hackerangriff

Was Sie erwartet Was tun, wenn es doch mal kracht? Die Erfahrung zeigt, wer vorbereitet ist, trifft im Ernstfall die [...]

online Webimpuls Angebot von CYBERSicher

Info & Anmeldung

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

IT-Sicherheitsdienstleister

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

Suche Qualifizierte IT-Dienstleister CyberRisikoCheck

Mit der Suchfunktion können Sie nach Namen, Ort oder PLZ filtern. Durch Eingabe von mehr oder weniger Buchstaben des Ortes bzw. des Namens oder Ziffern der PLZ können Sie Ihre Suche entsprechend einschränken oder ausweiten.

Ihnen ohne Sucheintrag, werden Ihnen alle eingetragenen "IT-Dienstleister" ausgegeben.



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

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

Fazit

Es wird passieren!

Weitere Informationen



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

Abschlussfragen

Was waren Ihre negativen
Reaktionsmaßnahmen?

War Ihr Unternehmen schon
mal Opfer eines
Cyberangriffs?

Was waren Ihre positiven
Reaktionsmaßnahmen?

VIELEN DANK

für Ihre Aufmerksamkeit!