CYBERsicher

IT-Sicherheit
IN DER WIRTSCHAFT

CYBERsicher Risikoradar

Wie sie den 6 wichtigsten Herausforderungen für kleine und mittlere Unternehmen begegnen können

Juni 2024

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital

Cybersicherheit in Deutschland

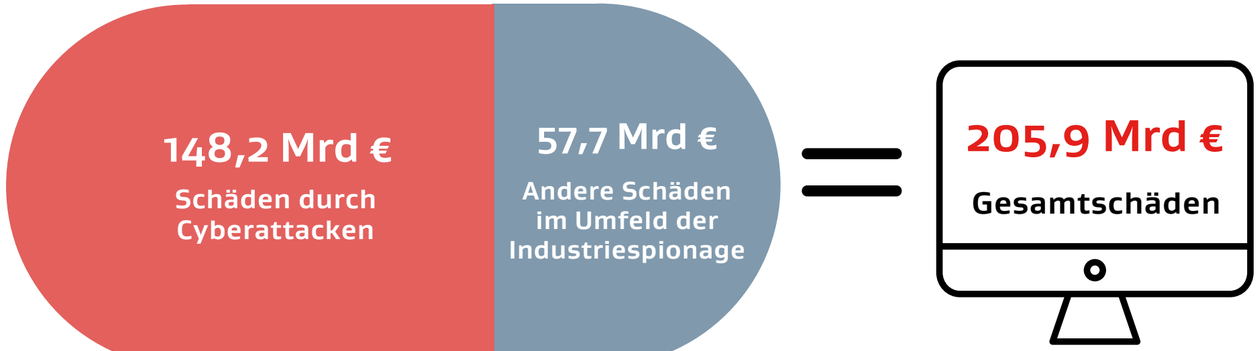
Die **zunehmende Digitalisierung** und Vernetzung ist Wirtschaftsmotor für Deutschland, ganz besonders in kleinen und mittleren Unternehmen. Doch das macht sie auch zu einem **attraktiven Ziel für Cyberkriminelle**. So geraten mittelständische Unternehmen immer häufiger in den Fokus.

In den letzten Jahren wurde jedes zweite Unternehmen mindestens einmal Ziel eines Cyberangriffs. [1]
Dabei geraten vor allem Lieferketten in den Fokus von Kriminellen.

Es ist wichtig, dass jedes Unternehmen das Thema Cybersicherheit strategisch anpackt und klare Richtlinien festlegt. Diese Verantwortung liegt bei der Unternehmensleitung.

Die Transferstelle bietet Ihnen Orientierung zu den ersten Schritten für Ihr Unternehmen – buchen Sie hierfür einfach einen **CYBER**Dialog:

CYBERDialoge ⟶



Quelle: [1] SoSafe GmbH. Human Risk Review 2023
Quelle Grafik: Bitkom: Dr. Wintergerst, Ralf. Wirtschaftsschutz 2023. Bitkom

Die wichtigsten Bedrohungen

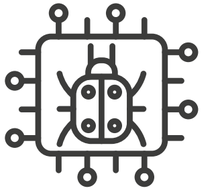
Die gefährlichsten Angriffsformen für Unternehmen in Deutschland

Welche Cyberangriffe haben in den letzten 12 Monaten Schaden verursacht?

31% Phishing

29% Angriffe auf Passwörter

28% Malware



23% Ransomware

Diese drei Teilbereiche der Cybersicherheit sollten Sie anpacken, um gut gewappnet zu sein:

Prävention

Zum Schutz des Unternehmens:
Cyberangriffe verhindern, bevor sie auftreten

Detektion

Zum Erkennen von IT-Sicherheitsvorfällen:
Vorfälle identifizieren, damit Maßnahmen ergriffen werden können

Reaktion

Zum Bekämpfen von Angriffen:
Um Schäden zu minimieren, ist eine schnelle und effektive Reaktion erforderlich

Quelle Grafik: Bitkom: Dr. Wintergerst, Ralf. Wirtschaftsschutz 2023. Bitkom

Worauf Sie sich vorbereiten müssen:

Cybersicherheit ist als fortlaufender Prozess im eigenen Unternehmen zu verstehen. Eine hundertprozentige Sicherheit kann es dabei nie geben. Die gute Nachricht: Sie können mit einigen **zielgerichteten Maßnahmen** die wichtigsten Einfallstore schließen.

Wir haben die **sechs wichtigsten Herausforderungen** für Sie zusammengestellt und geben Tipps, wie Sie die genannten Risiken richtig anpacken. Die verlinkten Angebote der Transferstelle Cybersicherheit im Mittelstand helfen Ihnen dabei.

Phishing-Angriffe erkennen und verhindern

1

Passwörter und Authentisierungs-daten absichern

2

Ransomware-Angriffe verhindern und überstehen

3

Ihr Team sensibilisieren

4

Angriffe auf die Software-Lieferkette verhindern

5

Ihre IT-Systeme sicher betreiben

6

Phishing-Angriffe erkennen und verhindern

Phishing ist eine Methode des Betrugs, bei der Angreifer:innen versuchen, **sensible Informationen zu erlangen**, indem sie sich in Nachrichten als vertrauenswürdig ausgeben. Betrüger:innen geben sich also zum Beispiel als Ihre Bank aus, um sich Zugangsdaten zu erschleichen.

Phishing-E-Mails stellen derzeit den verbreitetsten Zugangsweg für Ransomware-Angriffe dar. [2]

Jeder zweite User **(47%)** öffnet Phishing Mails

Jeder dritte User davon **(31%)** klickt den in der Mail enthaltenen schädlichen Inhalt an

Jeder zweite User davon **(52%)** interagiert weiter mit den Inhalten

Wie kann ich mein Unternehmen vor Phishing schützen?

Sensibilisieren Sie Ihre Mitarbeitenden regelmäßig für betrügerische Nachrichten und erklären Sie die Relevanz für Ihren Geschäftsbetrieb.

Kümmern Sie sich um die Grundlagen: Weisen Sie alle Teammitglieder in den richtigen und sicheren Umgang mit Informationstechnologien ein.

Nutzen Sie E-Mail-Filter, die vor Viren und E-Mails mit betrügerischer Absicht (SPAM) schützen.

Auf der Plattform der Transferstelle Cybersicherheit finden Sie Materialien zur Sensibilisierung ihrer Mitarbeitenden:

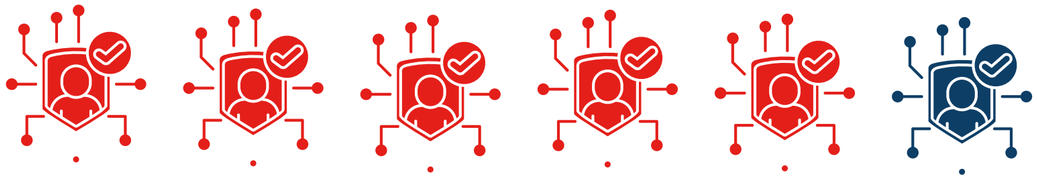
Materialien →

Quelle: [2] Cybercrime Bundeslagebild, Bundeslagebild 2022. Bundeskriminalamt
Quelle Grafik: SoSafe GmbH. Human Risk Review 2023

Passwörter und Authentisierungsdaten absichern

Sie sorgen dafür, dass bei einem Angriff das gesamte Netzwerk betroffen sein kann: Ein unsicheres Passwort öffnet nicht nur den Richtigen Tür und Tor, sondern auch Angreifer:innen.

Nutzen Sie ein unsicheres Passwort für mehrere Accounts, so können bei einem IT-Sicherheitsvorfall gleich mehrere Zugänge betroffen sein.



84% aller betrügerischen E-Mails zielten auf die Erbeutung von Authentisierungsdaten ab

Was kann mein Unternehmen gegen unsichere Passwörter tun?

- Erstellen Sie eine Richtlinie für sichere Passwörter – Passwörter sollten möglichst lang und komplex sein.
- Stellen Sie einen Passwortmanager bereit und verpflichten Sie Mitarbeitende auf seine Nutzung.
- Verwenden Sie Multifaktor-Authentisierung, wo möglich.

Auf der Seite der Transferstelle finden Sie Materialien, die Ihnen dabei helfen, Passwortrichtlinien einzuführen:

Materialien →

Quelle Grafik: Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Lage der IT-Sicherheit in Deutschland 2023

Ransomware-Angriffe verhindern und überstehen

Ransomware ist eine Art von Schadsoftware, die darauf abzielt, die Dateien der Betroffenen zu verschlüsseln oder den Zugriff auf wichtige Funktionen eines Systems oder Netzwerks zu sperren. Für die Freigabe wird dann **Lösegeld erpresst.**

Es gibt viele Wege, wie eine Ransomware Zugriff auf Ihr Unternehmen erhalten kann. In der Regel nutzen die Angreifer:innen dazu **Sicherheitsschwächen** aus. Kommt es zu einem erfolgreichen Angriff, helfen vorbereitende Maßnahmen, Schlimmeres zu verhindern.

Ransomware: Betroffene Unternehmen in Deutschland

- Kleine und Mittelständische Unternehmen
- Große Unternehmen

Wie kann ich mein Unternehmen auf Ransomware-Angriffe vorbereiten?

Verwenden Sie ein Virenschutzprogramm, eine Firewall und verschlüsselte VPN-Verbindungen.

Nutzen Sie aktuelle Hardware und Software mit automatischen Softwareaktualisierungen. Benennen Sie eine Person, die für diese Updates zuständig ist.

Fertigen Sie Sicherheitskopien an: Identifizieren Sie die unternehmenskritischen Daten, die gesichert werden sollen, und erstellen Sie regelmäßig Sicherungen (Backups). Diese sollten Sie getrennt lagern – so sind sie für Angreifer unzugänglich.

Auf der Plattform der Transferstelle finden Sie Materialien, die Ihnen dabei helfen, Ransomware-Angriffe zu verhindern und zu überstehen:

Materialien →

Quelle Grafik: Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Lage der IT-Sicherheit in Deutschland 2023

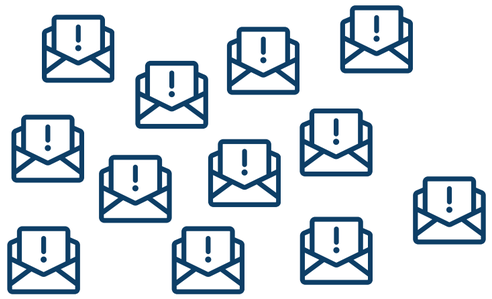
Ihr Team sensibilisieren

Der Faktor Mensch spielt beim Thema Cybersicherheit eine bedeutende Rolle. Durch eine Kultur des Bewusstseins für Cyberrisiken und durch sensibilisierte Mitarbeitende können Sie Ihr Unternehmen effektiv schützen.

Bei Organisationen, deren Führungskräfte für Cyberrisiken sensibilisiert sind, steigt die Wahrscheinlichkeit um 67 Prozent, dass sie ausreichende Mittel für Sicherheitsbelange bereitstellen. [3]

Anteil der Cyberangriffe durch menschliches Versehen an KMU, die von Cyberattacken betroffen waren.

Öffnen von Phishing-Mails, Herunterladen schädlicher Anhänge, Spam und falsche Identitäten:



2022: **56%**

2023: **48%**

Wie kann ich das Bewusstsein meiner Mitarbeitenden nachhaltig stärken?

- Kultur der IT-Hygiene: Schulen Sie Mitarbeitende regelmäßig zu guten Sicherheitspraktiken und den wichtigsten Bedrohungen.
- Erklären Sie transparent, warum diese Schulungen für den Geschäftsbetrieb so wichtig sind.
- Ermutigen Sie Mitarbeitende zum Melden von Vorfällen. Ziel soll es sein, eine positive Fehlerkultur im Umgang mit IT zu fördern.

Sensibilisieren Sie Ihre Mitarbeitenden spielerisch, mit Lernspielen zum Thema Cybersicherheit:

Materialien →

Quelle: [3] SoSafe GmbH. Human Risk Review 2023
Quelle Grafik: HDI Versicherungen. HDI Cyberstudie 2023

Angriffe auf die Software-Lieferkette verhindern

In den vergangenen 12 Monaten waren in der EU 61 Prozent der Unternehmen von einem Angriff auf ihre Software-Lieferkette betroffen. [4]

8 von 10 Sicherheitsverantwortlichen sagen, dass die Sicherheit ihrer Organisation zunehmend von der Sicherheit ihrer Partner und Lieferanten abhängt. [5]

Ein Supply-Chain-Angriff **nutzt Schwachstellen in der Lieferkette** aus, um Zugang zu den Systemen oder Daten eines Zielunternehmens zu erlangen. Damit kann ein Angriff auf Drittanbieter von Software leicht zu einem Angriff auf Ihr Unternehmen werden.

Wie kann ich mein Unternehmen vor Angriffen auf die Lieferkette schützen?

Machen Sie die Sicherheit Ihrer Lieferkette zu Ihrem Projekt: Investieren Sie Zeit und Personal darin, Ihre Lieferkette zu überblicken und Dienstleisterverhältnisse zu durchschauen.

Sorgen Sie dafür, dass die Person, die in Ihrem Unternehmen für die IT-Sicherheit verantwortlich ist, regelmäßig Rücksprache mit der Geschäftsführung hält.

Setzen Sie sich mit der NIS-2-Richtlinie auseinander und prüfen Sie, ob Sie davon betroffen sind.

Setzen Sie sich mit den Anforderungen des Cyber Resilience Act auseinander. Dieser beschreibt Cybersicherheitsanforderungen an Hard- und Softwareprodukte.

In unserem Artikel finden Sie eine Zusammenfassung der wichtigsten Eckpunkte zum Thema NIS-2:

Zum Artikel ⟶

Quelle: [4] European Union Agency for Cybersecurit. ENISA Threat Landscape 2023
Quelle: [5] SoSafe GmbH. Human Risk Review 2023

Ihre IT-Systeme sicher betreiben

Unternehmen in Deutschland fehlen aktuell 149.000 IT-Fachkräfte. [6]

IT-Systeme sind nicht pauschal sicher oder unsicher. Wie sie konkret konfiguriert und betrieben werden, entscheidet darüber, ob sie Opfer eines Angriffs werden.

Die Personen, die IT-Systeme administrieren, sollten neben ausreichender Zeit über ausreichende Fachkenntnisse verfügen und diese aktuell halten.

Wie können Sie sicherstellen, dass die IT-Systeme Ihres Unternehmens sicher administriert werden?

- Sorgen Sie dafür, dass Ihre Systeme regelmäßig aktualisiert werden (Updates).
- Sorgen Sie dafür, dass nur Administrator:innen über Administratorenrechte verfügen. Normale Nutzer:innen sollten nur Zugriff auf die absolut notwendigen Freigaben haben.
- Ihr Netzwerk sollte segmentiert sein. Damit ist die Aufteilung eines Netzwerks in kleinere, getrennte Teilnetze gemeint. Das verhindert, dass Angreifer:innen sich frei im gesamten Netzwerk bewegen.
- Sorgen Sie dafür, dass Daten nur verschlüsselt übermittelt werden. Dies können Sie zum Beispiel durch verschlüsselte E-Mails erreichen.

Schon gewusst? Der CyberRisiko-Check hilft kleinen Unternehmen die Grundlagen der Cybersicherheit gemeinsam mit einem IT-Dienstleister anzupacken. Mehr dazu unter:

Zum Check →

Quelle: [6] Der Arbeitsmarkt für IT-Fachkräfte (Bitkom)

Zukunfttrends

Neue Risiken durch Künstliche Intelligenz und das Internet der Dinge

Welche Cyberrisiken müssen kleine und mittlere Betriebe in Zukunft auf dem Schirm behalten?

Während digitale Zukunftstrends zahlreiche Potenziale für den Mittelstand bergen, können auch neue Gefahren entstehen.

37%

Der befragten Firmen hatten Cybersicherheitsvorfälle aufgrund von IoT-Produkten [7]

20%

Klicken auf KI-generierte Phishing-Mails [8]

Künstliche Intelligenz

Automatisierte soziale Manipulation (Social Engineering): KI-Sprachmodelle sind in der Lage, sehr schnell immer schwerer zu identifizierende Phishing-Nachrichten zu verfassen. Sie können auf menschliche Reaktionen antworten und so ihre Glaubwürdigkeit steigern. [9]

Dabei kommt auch vermehrt sogenanntes Vishing zum Einsatz: Ein paar Sekunden Audioaufnahme reichen aus, um eine überzeugende gefälschte Stimme zu erstellen. Cyberkriminelle nutzen dann KI, um Stimmen zu klonen und sich als Kolleg:innen oder Vorgesetzte auszugeben. [9]

Das Internet der Dinge

Über das Internet der Dinge (Internet of Things, kurz IoT) sind alltägliche Gegenstände mit dem Internet verbunden, wie z.B. Überwachungskameras. Viele dieser Geräte verfügen über keine ausreichende Sicherheit und können manipuliert werden.

Im industriellen Umfeld kommen oft auch vernetzte Systeme in der Produktion zum Einsatz. Diese müssen auch geschützt werden, denn große Teile der Infrastruktur hängen davon ab. [7]

Quelle Grafik: [7] Onekey GMBH. IOT Security Report 2022
Quelle Grafik: [8] SoSafe GmbH. Human Risk Review 2023
Quelle: [9] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Die Lage der IT-Sicherheit in Deutschland 2023*

IT-Sicherheit
IN DER WIRTSCHAFT

Wir machen den Mittelstand #CYBERsicher.

Die Transferstelle Cybersicherheit im Mittelstand unterstützt kleine und mittlere Unternehmen, Handwerksbetriebe und Start-Ups kostenfrei und anbieterneutral.

Unsere Angebote:

- Workshops und Veranstaltungen: Praxisorientierte Formate zum Thema Cybersicherheit – auf Ihr Unternehmen ausgerichtet
- Materialien: Wir bieten Leitfäden, Informationsbroschüren und Selbstlernangebote für Ihre Weiterbildung an
- Mit dem CYBERsicher Check jetzt schnell und einfach die IT-Sicherheit in Ihrem Unternehmen anpacken!
- Die CYBERsicher Notfallhilfe: Wenn es zum Vorfall kommt, finden Sie hier schnell und unkompliziert Hilfe (Start: Sommer 2024)

Besuchen Sie uns auf unserer Webseite
www.transferstelle-cybersicherheit.de

Mittelstand-Digital

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

Die Transferstelle Cybersicherheit im Mittelstand gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung und IT-Sicherheit in kleinen und mittleren Unternehmen.

Impressum
Der Mittelstand, BVMW e.V. | Potsdamer Straße 7 | 10785 Berlin |Vereinsregister Berlin Charlottenburg Nr. 19361 Nz | Ust.-ID-Nr. DE 230883382
Fachliche Erarbeitung: Dr. Dirk Achenbach (FZI Forschungszentrum Informatik), Sergio Marschall (FZI Forschungszentrum Informatik) - Text & Redaktion: Tamara Bayreuther (Der Mittelstand, BVMW e.V.), Tobias Diemer (Der Mittelstand, BVMW e.V.), Marc Dönges (Der Mittelstand, BVMW e.V.) | Verantwortlicher i.S.v. § 5 TMG: Lutz Kordges, Pressesprecher des BVMW | Vereinsregister Berlin Charlottenburg Nr. 19361 Nz | USt.-ID-Nr. DE 230883382 | Vertreten durch den Vorsitzenden der Bundesgeschäftsführung i.S.v. §26 BGB: Senator a. D. Christoph Ahlhaus | Design: Agentur Emilian | Stand: Juni 2024