Business Resilience im Kontext unternehmens-kritischer Cyberrisiken

Eine Studie der Hochschule München & der 4C GROUP AG

München, 2026

Cyberangriffe machen Business Resilience zu einer unternehmerischen Kernfähigkeit

334.000

Registrierte Cybercrime-Fälle in Deutschland im Jahr 2025[1]

Ransomware-Angriffe bleiben die zentrale Bedrohung, während ein deutlicher Anstieg von **DDoS-Angriffen** zu verzeichnen ist.

24 Tage

Ø Ausfallzeit nach Ransomware-Angriff in den USA[2]

Bis zur **Wiedererlangung einer 100-prozentigen Produktivität** erleiden die Organisationen erhebliche Umsatzeinbußen.

202,4 Mrd. €

Schaden durch Cyberattacken in Deutschland im Jahr 2025[1,3]

Das gesamte **Schadensvolumen** durch Cyberattacken entspricht damit rund **4,5 % des deutschen Bruttoinlandsprodukts**

Ziel der Studie ist es, herauszufinden, wie Maßnahmen nach Cyberangriffen so gestaltet und verankert werden können, dass diese wirksam zur Wiederherstellung des Geschäftsbetriebs und damit zur Steigerung der **Business Resilience** beitragen

*→ Im Kontext der Studie bedeutet **Business Resilience** die Fähigkeit einer Organisation, im Falle einer unerwarteten Störung flexibel zu bleiben und den Geschäftsbetrieb aufrechtzuerhalten, indem sie sich an die Situation anpasst*

[1]BMI, 2025
[2]Statista Research Department, 2022
[3]Bitkom Research Wirtschaftsschutz, 2025

Ausgangsszenario des Interviews

Ihr Unternehmen ist von einem schwerwiegenden Cyberangriff betroffen. Zentrale IT-Systeme sind nicht oder nur stark eingeschränkt verfügbar. Ein Großteil der Mitarbeitenden kann nicht mehr normal arbeiten. Kritische Geschäftsprozesse stehen still oder laufen nur noch manuell, mit erheblichen Effizienz- und Qualitätsverlusten. Die Ursache, das tatsächliche Schadensausmaß und die Dauer des Ausfalls sind aktuell unklar.

Fragen des Interviewleitfadens

1. Welche **Entscheidungen** treffen Sie in den ersten 24 Stunden und warum?
2. Welche **Herausforderungen** erwarten Sie bei der Wiederherstellung des Geschäftsbetriebs Ihres Unternehmens?
3. Wobei entstehen die größten **Verzögerungen** in der Wiederherstellung und was sind die Ursachen dafür?
4. **Wie gehen Sie grundsätzlich vor**, um den Geschäftsbetrieb wieder handlungsfähig zu machen?
5. Welche drei **Maßnahmen** leisten den größten Beitrag zur kurzfristigen Wiederherstellung des Geschäftsbetriebs?
6. Ab **wann** würden Sie den Geschäftsbetrieb als **wiederhergestellt** betrachten und gibt es definierte **Zielwerte**, an denen Sie das festmachen?
7. Welche organisatorischen **Voraussetzungen, Strukturen oder Verantwortlichkeiten** müssen verankert sein, damit Maßnahmen im Ernstfall wirksam greifen?
8. Welche **zentrale Investition** würden Sie tätigen, um die Resilienz Ihres Unternehmens zu steigern?

9

Branchen

Automobilzulieferer

Chemie

Gesundheit & Pharma

Industrie & Produktion

Handel, Logistik & Services

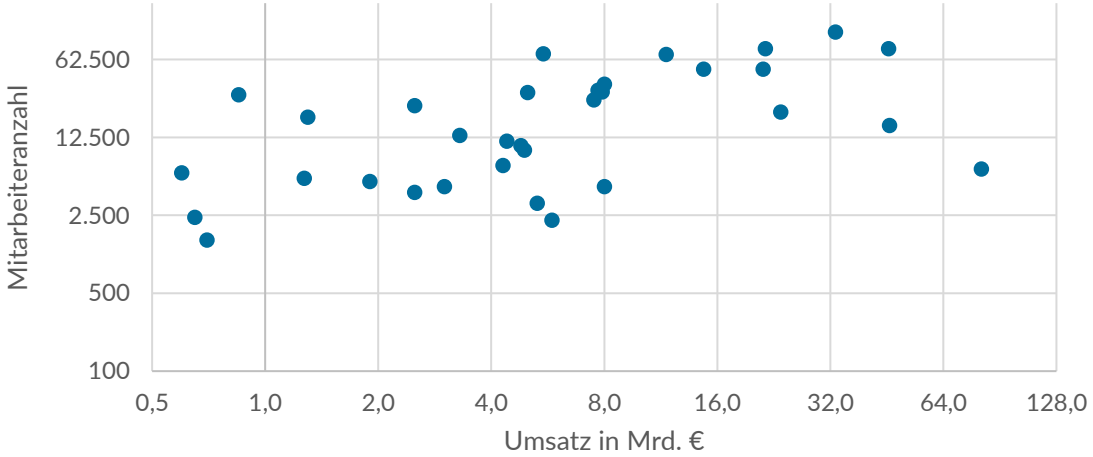
Konsumgüter

Finanzdienstleistungen

Öffentlicher Dienst

Versicherung

Unternehmen der Interviewteilnehmer:innen



Die 35 CIOs und IT-Entscheider der qualitativen Interviews sind in Unternehmen verschiedenster Branchen tätig. Die Unternehmen verzeichnen im Median einen **Umsatz von 5,15 Mrd. Euro*** und beschäftigen im Median **12.250 Mitarbeiter**.

*Der Median wird angegeben, da die Daten nicht normal verteilt sind und die Ausreißer den Mittelwert verzerren würden.

Vorgehen zur Wiederherstellung des Geschäftsbetriebs

Die Bewältigung eines Angriffs lässt sich in sechs Phasen gliedern, gefolgt von einer siebten Phase der Weiterentwicklung

Zusammenfassung & Ableitung: Welche Entscheidungen treffen Sie in den ersten 24 Stunden und warum? Wie gehen Sie grundsätzlich vor, um den Geschäftsbetrieb wieder handlungsfähig zu machen?
(n = 35)

Die Hälfte der CIOs sieht den Geschäftsbetrieb als wiederhergestellt an, wenn alle Kernprozesse wieder funktionsfähig sind

Kernprozesse wiederhergestellt (16 von 31) 1

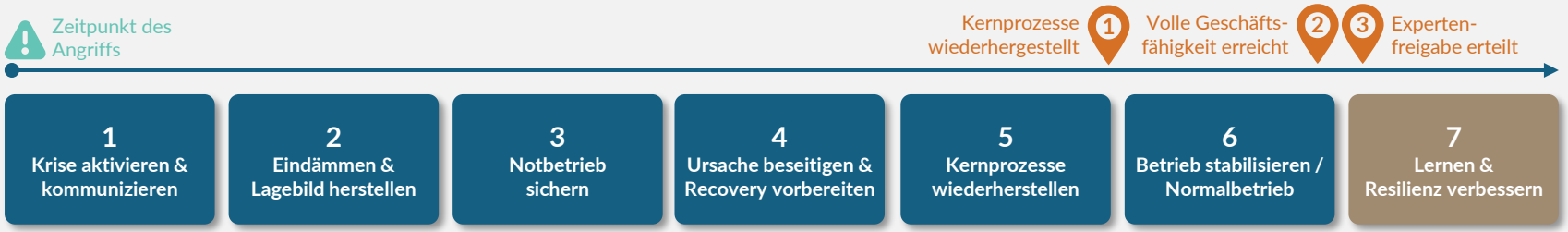
Geschäftsbetrieb wird als wiederhergestellt betrachtet, wenn die **wesentlichen oder kritischen Geschäftsprozesse** wieder funktionieren. Das bedeutet, dass das Unternehmen in der Lage ist, seine **Kernaufgaben zu erfüllen**, auch wenn noch nicht alle Systeme oder Prozesse vollständig wiederhergestellt sind.

Volle Geschäftsfähigkeit erreicht (10 von 31) 2

Erst wenn **alle Mitarbeiter wieder arbeiten** können, der Betrieb wieder im normalen Rahmen und mit **gewohnter Effizienz** läuft, wird der Geschäftsbetrieb als wiederhergestellt definiert. Dies beinhaltet, dass Dienstleistungen wieder angeboten werden können und der Betrieb den **Status vor dem Vorfall** erreicht.

Expertenfreigabe erteilt (5 von 31) 3

Einige betonen die **Notwendigkeit einer Expertenfreigabe**, beispielsweise durch Forensiker, bevor der Geschäftsbetrieb als wiederhergestellt gilt. Das umfasst umfangreiche Security-Tests, den **Nachweis**, dass der ursprüngliche Angriffsvektor behoben und geschlossen ist, sowie den Nachweis, dass die Systeme bereinigt sind.



Auswertung: Ab wann würden Sie den Geschäftsbetrieb als wiederhergestellt betrachten und gibt es definierte Zielwerte, an denen Sie das festmachen?
(n = 31)

Die erfolgreiche Wiederherstellung wird in den meisten Unternehmen nicht an messbaren Zielwerten festgemacht

80%

der 35 IT-Entscheider haben
keine Kennzahlen
für die Wiederherstellung definiert

Aktuell haben wir keine Zielwerte. Ich wüsste auch nicht, wie ich das quantitativ definieren sollte.“
– *CISO eines Mobilitäts- und Transportunternehmens*

„Wir haben kritische Systeme, die nach 4 Stunden wieder laufen müssen […] und businessrelevante Systeme, die auf 2 Tage ausgelegt sind. Danach folgen Stufen mit 10 Tage sowie 20 Tage Ausfallzeit.“
– *Head of Global IT eines Industrieunternehmens*

„Natürlich verwenden wir Kennzahlen, Systemverfügbarkeit [und] SLAs“
– *IT-Leitung im Gesundheitswesen*

54%

der 35 IT-Entscheider haben
RTOs & RPOs
für kritische Systeme definiert

„Die sind natürlich […] wichtig, aber auch extrem fehlleitend und es gibt unterschiedliche Sichtweisen. Das Business formuliert grundsätzlich ganz andere Ansprüche als das, was man in der IT tatsächlich leisten kann.“
– *CISO aus der Zulieferindustrie*

„[…] wir haben vertraglich RTO-/RPO-[Werte], also wie lange darf ein System ausfallen und wie schnell muss ein System wieder laufen.“
– *CISO eines Mobilitäts- und Transportunternehmens*

***RTO (Recovery Time Objective)**: Die maximale Zeitspanne, die der Wiederanlauf von Systemen nach einem Ausfall dauern darf*
***RPO (Recovery Point Objective)**: Die maximale Datenmenge, gemessen in der Zeit seit dem letzten Backup, die im Ernstfall verloren gehen darf*

Auswertung: Ab wann würden Sie den Geschäftsbetrieb als wiederhergestellt betrachten und gibt es definierte Zielwerte, an denen Sie das festmachen?
(n = 35)

Fehlende Vorbereitung, Transparenz und Priorisierung verursachen die größten Verzögerungen bei der Wiederherstellung

Auswertung & Ableitung: Welche Herausforderungen erwarten Sie bei der Wiederherstellung des Geschäftsbetriebs? Wobei entstehen die größten Verzögerungen und was sind die Ursachen dafür?
(n = 35)

Anhand von Maßnahmen lassen sich die Herausforderungen gezielten adressieren und den Reifegrad jeder Phase steigern

1 | Krise aktivieren & kommunizieren	2 | Eindämmen & Lagebild herstellen	3 | Notbetrieb sichern	4 | Ursache beseitigen & Recovery vorbereiten	5 | Kernprozesse wiederherstellen	6 | Betrieb stabilisieren & Normalbetrieb	7 | Lernen & Resilienz verbessern
Definierte Rollen & Governance Verantwortlichkeiten, Entscheidungsbefugnisse und Eskalationswege müssen vorab festgelegt und kommuniziert werden	**Festgelegte Dokumentation** Prozess-, Daten- und Abhängigkeitsinfor-mationen vollständig dokumentieren und verfügbar machen	**Out-of-Band-Kommunikation** Wenn E-Mail und Teams kompromittiert sind, bedarf es alternativer Kanäle. Diese müssen vorher definiert, getestet und bekannt sein	**Backup & Recovery-Strategien festlegen** Unveränderbare und getrennte Backups vorhalten. Entscheiden, wo die Backups liegen und in welcher Reihenfolge sie wiederhergestellt werden	**Business Impact Analyse durchführen** Kritische Prozesse identifizieren und deren maximale Ausfallzeiten definieren. Wer kritische Systeme nicht kennt, kann nicht sinnvoll handeln	**KPIs für Wiederher-stellung etablieren** Ab wann gilt der Geschäftsbetrieb als wiederhergestellt? Klare Definitionen an wann der Geschäftsbetrieb als wiederhergestellt gilt	**Lessons Learned einbauen** Nach jedem Vorfall und jeder Übung schauen, was hat funktioniert, was nicht? Diese Erkenntnisse dokumentieren und in die Pläne zurückspielen
Regelmäßige Tabletop-Exercises Szenarien gemeinsam durchspielen, ohne den operativen Betrieb zu unterbrechen und niederschwellig zu üben	**Segmentierung & Netzwerkarchitektur** Systeme müssen technisch in isolierbare Segmente unterteilt werden, um im Ernstfall schnell abtrennbar zu sein	**Notbetriebsumgebung aufbauen** Parallele Infrastrukturen und Out-of-Band-Kommunikationswege (separate Cloud oder Microsoft-Umgebung) vorbereiten	**Backup-Restore-Tests durchführen** Es muss getestet werden, wie lange die Wiederherstellung dauert und ob die Daten tatsächlich nutzbar sind. End-to-End-Tests sind hierbei nützlich	**Kritische Prozesse priorisieren** Welche Systeme müssen zuerst wieder laufen? Ohne klare Priorisierung entscheidet im Ernstfall der lauteste Rufer, nicht die Kritikalität	**Incident Response Plan & Playbooks** Anleitungen für definierte Szenarien, um impulsive Entscheidungen zu vermeiden. Als strategisches Rahmenwerk verstehen, nicht als starres Skript	**Kontinuierliche Verbesserung leben** Resilienz ist kein abzuschließendes Projekt, Insb. Bedrohungslagen, und Regulatorik ändern sich ständig. Maßnahmen müssen stetig aktualisiert werden.
Krisenstabsübungen abhalten Die Krisenorganisation als Ganzes trainieren, nicht nur IT-Mitarbeitende, sondern mit Management, HR, Kommunikation und Fachbereichen			**Interne Kompetenzen aufbauen** Interne Forensik Kapazität & -kompetenz aufbauen, oder alternativ skalierbare externe Unterstützung sicherstellen		**Rückführung in den Normalbetrieb testen** Übergang vom Notbetrieb zurück in die reguläre Systemlandschaft muss aktiv geübt werden	**Externe Expertise gezielt einbinden** Wo interne Ressourcen, Zeit oder Reichweite nicht ausreichen, externe Anbieter einbinden, um Qualität Glaubwürdigkeit sicherzustellen

Organisation *Personal* *Technik*

Zusammenfassung & Ableitung: Welche organisatorischen Voraussetzungen, Strukturen oder Verantwortlichkeiten müssen verankert sein, damit Maßnahmen im Ernstfall wirksam greifen?
(n = 35)

Die Mehrheit der CIOs legt den Fokus auf Prävention und betont zugleich, dass sie ohne Reaktionsfähigkeit nicht ausreicht

53%

Präventive Maßnahmen sind wichtiger

„Ich würde die Prävention etwas wichtiger. Ich muss zuerst sicherstellen, dass der Krisenfall gar nicht eintreten kann oder dass die Wahrscheinlichkeit dafür so gering wie möglich ist.“

– CIO einer Krankenversicherung

„Für mich ist die Prävention wichtiger. Mit einer guten Prävention brauche ich die Reaktion im besten Fall gar nicht.“

– Manager Informationssicherheit eines Industriekonzerns

41%

Prävention und Reaktion sind gleichrangig

„Wenn ich nur auf Prävention setze und es tatsächlich passiert, herrscht Headless Chicken Modus, und das geht nicht gut aus. Erfolgreiche Unternehmen haben immer die Balance im Blick.“

- Lead Resilience Officer eines Industriekonzerns

„Reine Prävention gab es in den 90ern: Firewall aufstellen, fertig. Das funktioniert heute nicht mehr, ein Angriff kommt irgendwann durch. Und Detektion ohne vernünftige Reaktion hilft nicht weiter.“

– Bereichsleiter IT-Sicherheit einer Versicherung

6%

Reaktive Maßnahmen sind wichtiger

„Vorbereitung und Prävention sind schon wichtig, aber der Schwerpunkt muss auf der Recovery-Fähigkeit liegen.

Ich würde immer wirklich in die Fähigkeiten investieren, unter Druck kontrolliert und schnell wieder arbeitsfähig zu werden.

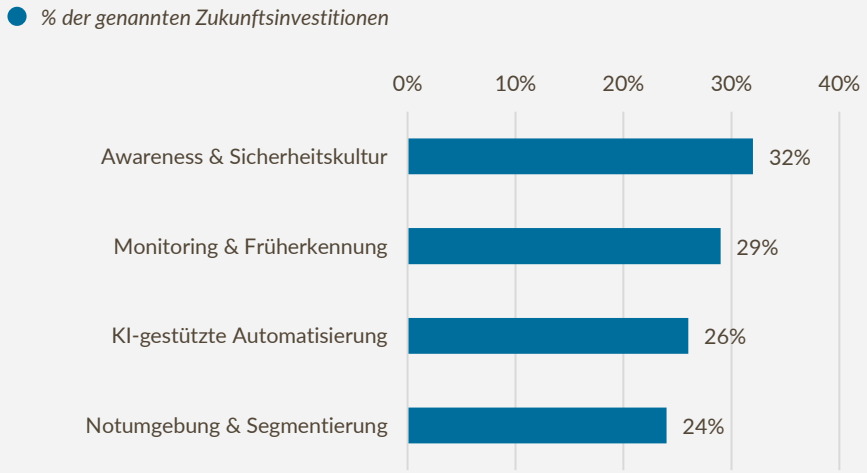
Das ist das, was ich gelernt habe, und es ist eigentlich meine persönliche Erfahrung aus dem, was uns passiert ist, und was total wichtig ist.“

– IT-Leitung im Gesundheitswesen

Die Mehrheit der IT-Entscheider **priorisiert Prävention** oder betrachtet **Prävention und Reaktion als gleichrangig**, allerdings nicht im Sinne reiner Abwehr. Beide Aspekte bedingen sich gegenseitig und bilden einen Kreislauf: Wer ausschließlich auf Prävention setzt, riskiert im Ernstfall unkoordiniertes Vorgehen.

Was ist Ihnen wichtiger: Die Prävention oder die Reaktion?
(n = 18)

Die IT-Entscheider wollen insbesondere in Awareness und Sicherheitskultur investieren



Auswertung: Welche zentrale Investition würden Sie tätigen, um die Resilienz Ihres Unternehmens zu steigern?
(n = 35); Mehrfachnennung möglich

Bei der Frage nach der zentralen Investition zur Steigerung der Resilienz zeigt sich, dass die IT-Entscheider deutlich über reine Technikbeschaffung hinausdenken und den **Menschen** sowie die **organisatorische Vorbereitung** als **kritische Faktoren** einstufen.

32% der CIOs würden primär in **Awareness und Sicherheitskultur** investieren, da fehlendes Problembewusstsein trotz technischer Schutzmaßnahmen eine zentrale Schwachstelle bleibt. Statt isolierter Schulungen und Phishing-Simulationen setzen sie auf eine Culture Journey in der IT-Entscheider sichtbar mitwirken.

29% priorisieren **Monitoring und Früherkennung**, etwa durch neue SIEM oder EDR Systeme. Für sie beginnt schnelle Reaktionsfähigkeit mit der frühzeitigen Identifikation von Anomalien, da nur so genug Zeit für eine koordinierte Reaktion bleibt.

26% setzen auf **KI gestützte Automatisierung**, insbesondere um die Incident Response zu beschleunigen und fehleranfällige manuelle Schritte bei der Bewältigung von Vorfällen zu reduzieren.

24% planen in eine getrennte **Notumgebung und Netzwerksegmentierung** investieren, um im Ernstfall einzelne Geschäftsbereiche gezielt isolieren und so eine Ausbreitung von Angriffen wirksam eindämmen zu können.

Sie möchten mehr über die Studie erfahren? Sprechen Sie uns gerne an!

Hochschule München

Alina Schwaiger
Masterandin
alina.schwaiger@hm.edu
+49 15783800873

Jessica Slamka
Professorin für IT-Management
jessica.slamka@hm.edu
+49 89 1265-2741

4C GROUP AG - Praxispartner

Patrick Hillebrand
Managing Consultant 4C
patrick.hillebrand@4cgroup.com
49 173 3465860

Martin Stephany
Senior Partner 4C
martin.stephany@4cgroup.com
+49 173 3465829

Impressum

4C GROUP AG

Office München
Elsenheimerstraße 55a
80687 München

Office Frankfurt
Senckenberganlage 19
60325 Frankfurt

Office Düsseldorf
Sky Office, Kennedydamm 24
40476 Düsseldorf

Office Berlin
Französische Straße 8
10117 Berlin

4cgroup.com