Conperience

WHITEPAPER FÜR ENTSCHEIDER

Vorbereitet, wenn es zählt.

Der Leitfaden für Entscheider zu IT-Notfallplan und Incident Response Plan – mit den häufigsten Fehlern, klaren Empfehlungen und einer Notfallkarte zum Mitnehmen.



IT-Notfallplan | Incident Response | Krisenstab | NIS2

Ausgabe 2026 · www.conperience.com

MANAGEMENT SUMMARY

Die Kernaussagen auf einer Seite

Ein Notfall ist der falsche Moment, um einen Plan zu schreiben. In den ersten Stunden entscheidet sich, ob aus einem Vorfall eine Krise wird – und das hängt fast vollständig von der Vorbereitung ab.

01 **Die ersten Stunden entscheiden.**

Ohne Plan wird improvisiert: Zeit geht verloren, Beweise werden vernichtet, Fehlentscheidungen vergrößern den Schaden.

02 **Die meisten Unternehmen haben die gleichen Lücken.**

Unklare Zuständigkeiten, Pläne nur digital, ungetestete Backups und keine Regeln für die Kommunikation.

03 **Zwei Pläne, ein Ziel.**

Der IT-Notfallplan bringt die IT zurück, der Incident Response Plan regelt die Reaktion auf Angriffe – beide sind Teil des Business Continuity Managements.

04 **Der Krisenstab braucht klare Rollen.**

Wer entscheidet, wer kommuniziert, wer koordiniert die Technik – festgelegt, bevor es ernst wird.

05 **Meldepflichten laufen ab Stunde null.**

DSGVO und NIS2 sehen kurze Fristen vor. Wer sie nicht kennt, riskiert zusätzliche Sanktionen.

06 **Ein Plan, der nicht geübt wird, funktioniert nicht.**

Planspiele und Wiederherstellungstests machen aus Papier echte Handlungsfähigkeit.

07 **Der Aufwand ist überschaubar.**

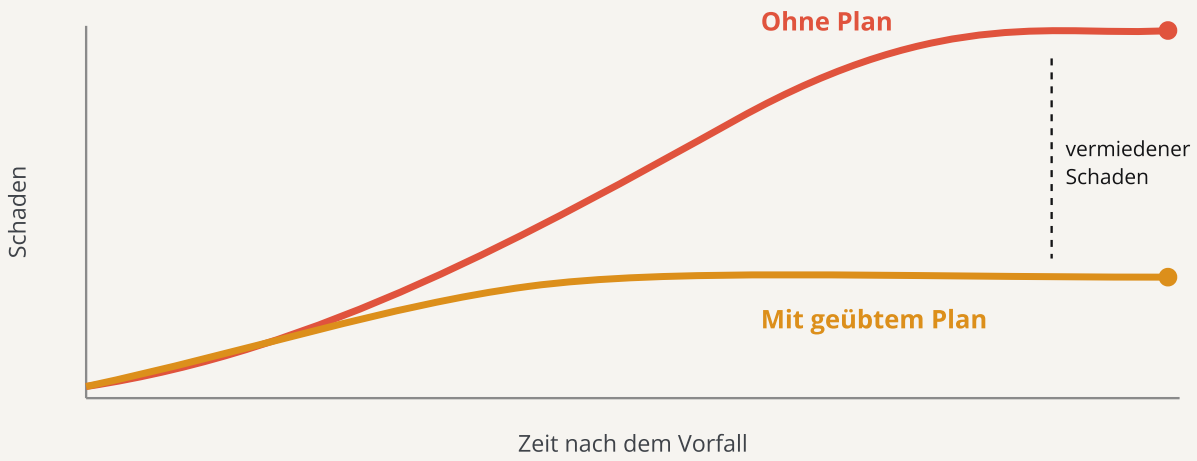
Mit einem strukturierten Vorgehen entstehen belastbare Pläne in wenigen Wochen – auch im Mittelstand.

01 WARUM VORBEREITUNG ENTSCHEIDET

Montag, 7:30 Uhr – nichts geht mehr

Die ersten Mitarbeitenden melden sich: keine Anmeldung möglich, auf den Bildschirmen eine Lösegeldforderung. Was jetzt passiert, entscheidet über das Ausmaß des Schadens.

Ohne Plan beginnt die Improvisation: Wer darf entscheiden? Wen rufen wir an? Dürfen wir die Systeme abschalten – oder vernichten wir damit Beweise? Sind die Backups noch intakt? Jede offene Frage kostet Zeit, und mit jeder Stunde wächst der Schaden.



Schematische Darstellung: Mit einem geübten Plan wird der Vorfall früher eingedämmt und der Betrieb schneller wiederhergestellt.

Zeit

Klare Abläufe sparen in den ersten Stunden wertvolle Zeit – oft die entscheidende.

Schaden

Schnelle Eindämmung begrenzt, wie viele Systeme und Daten betroffen sind.

Haftung

Dokumentierte Vorsorge schützt die Geschäftsleitung und erfüllt Pflichten aus NIS2.

02 DIE HÄUFIGSTEN PROBLEME

Sieben Lücken, die wir immer wieder sehen

In vielen Unternehmen gibt es zwar einzelne Vorkehrungen – aber keinen Plan, der im Ernstfall trägt. Diese Probleme begegnen uns am häufigsten:

01 Niemand weiß, wer entscheidet

Im Ernstfall diskutieren alle – und niemand hat das Mandat, Systeme abzuschalten oder Dienstleister zu beauftragen.

Empfehlung: Krisenstab mit klaren Rollen und Vertretungen benennen.

02 Der Plan liegt auf dem verschlüsselten Server

Notfallpläne, Kontaktlisten und Passwörter sind nur digital vorhanden – genau dort, wo der Angriff stattfindet.

Empfehlung: Notfallhandbuch und Kontaktlisten zusätzlich auf Papier und offline vorhalten.

03 Die Backups wurden nie getestet

Die Sicherung läuft – doch ob und wie schnell sich die Systeme wiederherstellen lassen, weiß niemand.

Empfehlung: Wiederherstellung regelmäßig testen und die Dauer messen.

04 Keine Prioritäten

Alles soll gleichzeitig zurückkommen. Ohne festgelegte Reihenfolge verzetteln sich die Teams.

Empfehlung: Kritische Prozesse und Wiederanlaufreihenfolge vorab festlegen.

05 Beweise werden vernichtet

Aus Panik werden Systeme sofort neu installiert – und mit ihnen die Spuren, die zeigen, wie der Angreifer hereinkam.

Empfehlung: Regeln zur Beweissicherung und Kontakte zu Forensik-Experten vorbereiten.

06 Kommunikation ohne Plan

Kunden erfahren es aus der Presse, Mitarbeitende spekulieren, Meldefristen werden verpasst.

Empfehlung: Kommunikationsplan mit Textbausteinen und Meldewegen erstellen.

07 Der Plan ist veraltet

Einmal erstellt, nie aktualisiert: Telefonnummern stimmen nicht mehr, Systeme haben sich geändert.

Empfehlung: Plan jährlich und nach jeder größeren Änderung prüfen und üben.

03 DIE EINORDNUNG

BCM, IT-Notfallplan und Incident Response – was ist was?

Die Begriffe werden oft vermischt. Dabei beantworten sie unterschiedliche Fragen – und greifen wie Zahnräder ineinander.

BUSINESS CONTINUITY MANAGEMENT

Wie läuft unser Geschäft weiter – egal, was passiert?

Der übergeordnete Rahmen für das ganze Unternehmen: kritische Prozesse, Notbetrieb, Krisenstab und Krisenkommunikation – auch für Ausfälle von Personal, Gebäuden oder Lieferanten.

IT-NOTFALLPLAN

Wie bringen wir die IT schnell und geordnet zurück?

Alarmierung, Wiederanlaufreihenfolge und Schritt-für-Schritt-Anleitungen für den Ausfall von Systemen – unabhängig von der Ursache.

INCIDENT RESPONSE PLAN

Wie reagieren wir auf einen Sicherheitsvorfall?

Erkennen, eindämmen, Beweise sichern, Angreifer entfernen und sicher wiederanlaufen – speziell für Cyberangriffe.

	IT-Notfallplan	Incident Response Plan
Auslöser	Jeder IT-Ausfall: Defekt, Brand, Stromausfall, Angriff	Sicherheitsvorfall: Angriff, Datenabfluss, Schadsoftware
Ziel	Betrieb schnell wiederherstellen	Angriff stoppen, Schaden begrenzen, sicher wiederanlaufen
Besonderheit	Wiederanlaufreihenfolge und Ersatzlösungen	Beweissicherung, Forensik, Meldepflichten
Beteiligte	IT, Fachbereiche, Dienstleister	Zusätzlich Forensik, Recht, Datenschutz, Behörden

Orientierung bieten anerkannte Standards wie der BSI-Standard 200-4 zum Business Continuity Management und die ISO 22301.

04 DER IT-NOTFALLPLAN

Acht Bausteine, die in keinen Plan fehlen dürfen

Ein guter Notfallplan ist kurz, verständlich und auch dann nutzbar, wenn die IT nicht funktioniert.

01
Notfallorganisation
Krisenstab, Rollen, Vertretungen und Entscheidungsbefugnisse.

02
Alarmierung
Kriterien für einen Notfall und eine Alarmierungskette – auch nachts.

03
Prioritäten
Kritische Prozesse, tragbare Ausfallzeiten (RTO) und Datenverluste (RPO).

04
Dokumentation
Systeme, Abhängigkeiten, Zugänge – vom Groben ins Feine.

05
Wiederanlaufpläne
Schritt-für-Schritt-Anleitungen, abgestimmt auf die Datensicherung.

06
Notfallhandbuch
Kompakt, auf Papier verfügbar, ergänzt um Notfallkarten.

07
Dienstleister
Verbindliche Zusagen zu Erreichbarkeit und Reaktionszeit.

08
Kommunikation
Wer informiert wann wen – mit vorbereiteten Textbausteinen.

Faustregel: Wenn jemand, der den Plan zum ersten Mal liest, in den ersten 30 Minuten eines Notfalls nicht weiß, was zu tun ist, ist der Plan zu kompliziert.

Was zusätzlich in den Plan gehört

- ✓ Liste der Zugangsdaten für Notfälle – sicher verwahrt, aber im Ernstfall erreichbar
- ✓ Ausweichmöglichkeiten: Arbeitsplätze, Kommunikationswege, Ersatzhardware
- ✓ Kontaktdaten von Versicherung, Polizei (Zentrale Ansprechstellen Cybercrime) und Datenschutzbehörde

05 ROLLEN IM ERNSTFALL

Der Krisenstab: Wer entscheidet, wer handelt

Im Ernstfall braucht es eine kleine, handlungsfähige Gruppe mit klarem Mandat – nicht eine große Runde ohne Entscheidungsbefugnis.



Was vorab geregelt sein muss

- Wer darf Systeme abschalten oder vom Netz nehmen?
- Wer darf externe Dienstleister und Forensiker beauftragen – und bis zu welchem Budget?
- Wer spricht mit Presse, Kunden und Behörden?
- Wer vertritt wen – auch im Urlaub und nachts?
- Wo trifft sich der Krisenstab, wenn das Gebäude oder die IT nicht verfügbar ist?
- Über welchen Kanal wird kommuniziert, wenn E-Mail ausfällt?

06 DER INCIDENT RESPONSE PLAN

Sechs Phasen der Reaktion auf einen Angriff

Ein Cyberangriff ist mehr als ein Ausfall: Angreifer können noch aktiv sein, Daten abfließen, Beweise verloren gehen. Der Incident Response Plan führt Schritt für Schritt durch die Reaktion.



1 **Vorbereiten**
Rollen, Werkzeuge, Kontakte zu Experten und geübte Abläufe.

2 **Erkennen und bewerten**
Echter Vorfall? Wie schwer? Welche Daten? Meldepflichten?

3 **Eindämmen**
Systeme isolieren, Konten sperren – ohne Spuren zu vernichten.

4 **Analysieren und beseitigen**
Einstiegspunkt finden, Ausmaß erheben, Angreifer vollständig entfernen.

5 **Sicher wiederherstellen**
Aus sauberen Sicherungen, mit neuen Zugängen, kontrolliert.

6 **Nachbereiten und lernen**
Lehren ziehen, Pläne und Schutzmaßnahmen verbessern.

Beweissicherung nicht vergessen: Wer vorschnell neu installiert, vernichtet die Spuren, die zeigen, wie der Angreifer hereinkam – und ob er noch da ist. Für eine gerichtsverwertbare Analyse braucht es eine saubere Sicherung der betroffenen Systeme.

07 DIE ERSTEN 72 STUNDEN

Was wann zu tun ist

Ein Notfall verläuft in Wellen. Diese Übersicht zeigt, worauf es in den einzelnen Phasen ankommt – als Orientierung für Ihren eigenen Plan.

0–1 h
Ruhe und Überblick

- Vorfall melden, Krisenstab alarmieren
- Betroffene Systeme isolieren
- Backups schützen
- Erste Fakten dokumentieren

1–4 h
Lage bewerten

- Ausmaß und Art des Vorfalls einschätzen
- Experten und Dienstleister hinzuziehen
- Meldepflichten prüfen
- Interne Erstinformation

4–24 h
Eindämmen und planen

- Angriff stoppen, Zugänge sperren
- Beweise sichern
- Wiederanlauf priorisieren
- Fristgerechte Meldungen vorbereiten

24–72 h
Wiederanlauf

- Kritische Systeme aus sauberen Backups
- Notbetrieb für wichtige Prozesse
- Kunden und Partner informieren
- Laufende Dokumentation

Dokumentieren Sie alles

Jede Maßnahme mit Uhrzeit und Verantwortlichem. Das hilft bei Forensik, Versicherung und Meldungen.

Kein Kontakt zu Erpressern ohne Plan

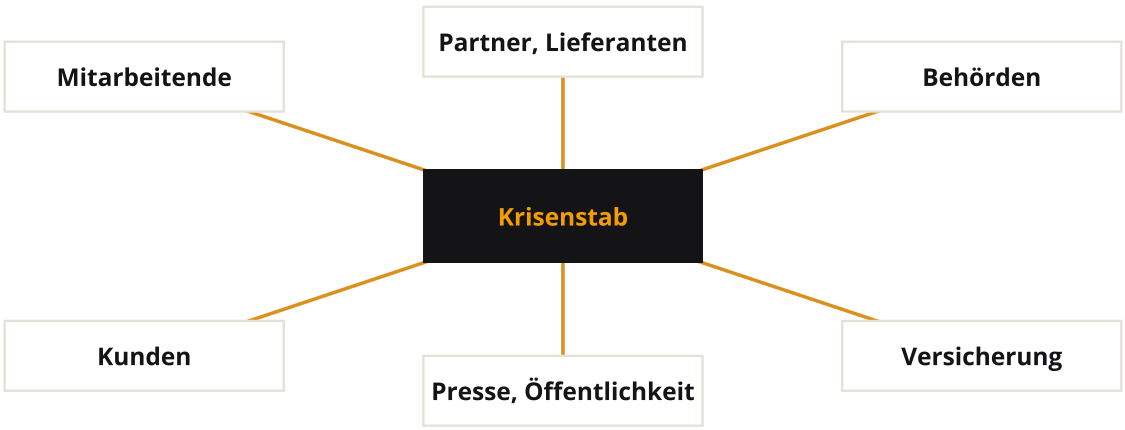
Ob und wie verhandelt wird, entscheidet der Krisenstab mit Experten – nie spontan.

Kräfte einteilen

Ein Notfall dauert oft Tage. Schichten und Pausen gehören in den Plan.

08 KOMMUNIKATION UND MELDEPFLICHTEN

Richtig kommunizieren, wenn nichts mehr funktioniert



Wer muss wann informiert werden? Diese Frage sollte für jede Gruppe vorab beantwortet sein.

Meldepflichten im Blick behalten

Bei Datenschutzverletzungen und erheblichen Sicherheitsvorfällen gelten gesetzliche Meldefristen. Für betroffene Unternehmen sind insbesondere diese relevant:

24 h
NIS2: Frühwarnung an die zuständige Behörde nach Kenntnis eines erheblichen Sicherheitsvorfalls

72 h
NIS2: Meldung mit erster Bewertung · DSGVO: Meldung einer Datenschutzverletzung an die Aufsichtsbehörde

1 Monat
NIS2: Abschlussbericht zum Vorfall

Ob und welche Pflichten für Ihr Unternehmen gelten, hängt von Branche, Größe und Art des Vorfalls ab. Diese Übersicht ersetzt keine Rechtsberatung.

Damit Kommunikation auch ohne IT funktioniert

- ✓ Mehrere unabhängige Kanäle: Mobilfunk, Festnetz, im Zweifel Messenger auf privaten Geräten nach festen Regeln
- ✓ Kontaktlisten und vorbereitete Textbausteine auf Papier

09 SO ENTSTEHT IHR PLAN

In sieben Phasen zum belastbaren Notfallplan

Ein Notfallplan entsteht nicht am Schreibtisch der IT, sondern im Zusammenspiel von Geschäftsführung, Fachbereichen und Technik.

A	**Analyse und Business-Impact-Analyse** Kritische Prozesse, Systeme und Abhängigkeiten erfassen; tragbare Ausfallzeiten und Datenverluste festlegen.	ERGEBNIS Prioritätenliste mit RTO/RPO
B	**Leitlinie und Notfallorganisation** Ziele, Verantwortung und Ressourcen mit der Geschäftsleitung festlegen; Krisenstab benennen.	ERGEBNIS Freigegebene Leitlinie, Rollen
C	**IT-Notfallplan** Alarmierung, Meldewege, Wiederanlaufreihenfolge und Anleitungen erarbeiten.	ERGEBNIS IT-Notfallplan
D	**Incident Response Plan** Abläufe für Sicherheitsvorfälle inklusive Beweissicherung, Meldepflichten und Expertenkontakten.	ERGEBNIS Incident Response Plan
E	**Notfallhandbuch und Kommunikation** Alles kompakt zusammenführen, Notfallkarten und Textbausteine erstellen, Papierversion verteilen.	ERGEBNIS Handbuch, Notfallkarten
F	**Schulung und Übungen** Verantwortliche schulen, Planspiele mit der Geschäftsleitung, echte Wiederherstellungstests.	ERGEBNIS Geübte Abläufe, Testprotokolle
Z	**Pflege und Verbesserung** Jährliche Überprüfung, Aktualisierung nach Änderungen, Erkenntnisse aus Übungen einarbeiten.	ERGEBNIS Lebendiges Notfallmanagement

10 TIPPS AUS DER PRAXIS

Do & Don't bei der Notfallplanung

Das sollten Sie tun

- ✓ Klein anfangen: zuerst die kritischsten Prozesse absichern
- ✓ Den Plan kurz halten – Checklisten statt Romane
- ✓ Papierversion an mehreren Orten aufbewahren
- ✓ Vertretungen für jede Rolle benennen
- ✓ Dienstleister vertraglich einbinden
- ✓ Mindestens einmal im Jahr üben – mit der Geschäftsleitung
- ✓ Nach jeder Übung und jedem Vorfall den Plan verbessern
- ✓ Versicherung und Notfallplan aufeinander abstimmen

Das sollten Sie vermeiden

- ✗ Den Plan allein der IT überlassen
- ✗ Pläne nur auf Systemen speichern, die ausfallen können
- ✗ Ungetestete Backups als Sicherheit betrachten
- ✗ Im Ernstfall Systeme vorschnell neu installieren
- ✗ Ohne Abstimmung mit Erpressern Kontakt aufnehmen
- ✗ Kunden und Mitarbeitende im Unklaren lassen
- ✗ Meldefristen erst im Ernstfall recherchieren
- ✗ Den Plan einmal schreiben und dann vergessen

Unser wichtigster Rat: Ein einfacher Plan, der geübt ist, schlägt jeden perfekten Plan, den niemand kennt. Beginnen Sie mit einem Planspiel am Besprechungstisch – in wenigen Stunden zeigt sich, wo die größten Lücken liegen.

ZUM MITNEHMEN

Ihre Notfallkarte: Die ersten 60 Minuten

Drucken Sie diese Seite aus, ergänzen Sie die Kontaktfelder und legen Sie sie dort ab, wo sie im Ernstfall gefunden wird – nicht nur digital.

IT-Notfall? Ruhe bewahren.

NOTFALLKARTE

1. **Nicht übereilt handeln**
   Keine Systeme neu starten oder neu installieren. Nichts löschen.
2. **Vorfall melden**
   Sofort an die Notfall-Hotline bzw. den Notfallmanager (siehe unten).
3. **Betroffene Geräte isolieren**
   Netzwerkkabel ziehen bzw. WLAN trennen – Gerät eingeschaltet lassen.
4. **Krisenstab alarmieren**
   Leitung, Notfallmanager, IT, Kommunikation – laut Alarmierungsliste.
5. **Backups schützen**
   Sicherungssysteme vom Netz trennen, Zugänge sperren.
6. **Alles dokumentieren**
   Was, wann, wer, welche Beobachtungen – mit Uhrzeit, gern mit Fotos.
7. **Experten hinzuziehen**
   IT-Dienstleister, Forensik, ggf. Versicherung und Polizei.
8. **Meldepflichten prüfen**
   Datenschutz und NIS2: Fristen laufen ab Kenntnis des Vorfalls.
9. **Intern informieren**
   Kurze, abgestimmte Information an die Mitarbeitenden.
10. **Nicht auf Erpresser reagieren**
    Jeder Kontakt nur nach Entscheidung des Krisenstabs.

NOTFALLMANAGER · TELEFON	IT-DIENSTLEISTER · HOTLINE	CYBERVERSICHERUNG · HOTLINE
LEITUNG KRISENSTAB · TELEFON	DATENSCHUTZBEAUFTRAGTE(R)	TREFFPUNKT KRISENSTAB

11 SELBSTCHECK

Wie gut ist Ihr Unternehmen vorbereitet?

Zählen Sie für jedes „Ja“ zwei Punkte, für „Teilweise“ einen Punkt.

01	Gibt es einen aktuellen IT-Notfallplan, der auch auf Papier verfügbar ist?	☐ Ja	☐ Teilw.	☐ Nein
02	Ist ein Krisenstab mit Rollen und Vertretungen benannt?	☐ Ja	☐ Teilw.	☐ Nein
03	Ist geregelt, wer Systeme abschalten und Experten beauftragen darf?	☐ Ja	☐ Teilw.	☐ Nein
04	Gibt es einen Plan speziell für Cyberangriffe, inklusive Beweissicherung?	☐ Ja	☐ Teilw.	☐ Nein
05	Wissen wir, welche Systeme zuerst wieder laufen müssen?	☐ Ja	☐ Teilw.	☐ Nein
06	Wurde die Wiederherstellung in den letzten zwölf Monaten getestet?	☐ Ja	☐ Teilw.	☐ Nein
07	Kennen wir unsere Meldepflichten und die Fristen?	☐ Ja	☐ Teilw.	☐ Nein
08	Gibt es einen Kommunikationsplan mit vorbereiteten Texten?	☐ Ja	☐ Teilw.	☐ Nein
09	Sind Dienstleister für den Notfall vertraglich eingebunden?	☐ Ja	☐ Teilw.	☐ Nein
10	Hat die Geschäftsleitung den Ernstfall schon einmal geübt?	☐ Ja	☐ Teilw.	☐ Nein

16–20 Punkte

Gut vorbereitet. Halten Sie Ihren Plan durch Übungen lebendig.

9–15 Punkte

Gute Ansätze mit Lücken. Schließen Sie die offenen Punkte gezielt.

0–8 Punkte

Dringender Handlungsbedarf. Beginnen Sie mit Krisenstab und Notfallkarte.

ÜBER CONPERIENCE

Wir beraten – oder erstellen Ihre Pläne komplett.

Von A bis Z: Wir passen uns an Ihre Ressourcen und Ihren Reifegrad an – herstellerneutral und pragmatisch.

VARIANTE 1

Wir beraten und begleiten

Ihr Team erarbeitet die Pläne, wir liefern Methodik, Vorlagen und Erfahrung, moderieren Workshops und prüfen die Ergebnisse.

VARIANTE 2

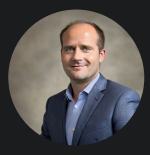
Wir erstellen für Sie

Wir übernehmen IT-Notfallplan, Incident Response Plan und Notfallhandbuch komplett – Sie geben die Inhalte frei.

Hinter uns steht ein großes Team erfahrener Spezialistinnen und Spezialisten – von Business Continuity Management, NIS2 und ISO-Zertifizierung bis zur Netzwerk- und Sicherheitstechnik. Als unabhängiger Partner für Technologie, Architektur, Resilienz und Datensouveränität empfehlen wir, was zu Ihrem Unternehmen passt.



Christian Habel
Gründer & Geschäftsführer



Andreas Habel
Gründer & Geschäftsführer

TELEFON
(+49) 040 607 74 74 - 0

E-MAIL
info@conperience.com

WEB
www.conperience.com

Conperience GmbH · Burgblick 26 · 55595 Gutenberg · © 2026. Alle Angaben ohne Gewähr; dieses Whitepaper ersetzt keine Rechtsberatung.