Checkliste für Inhaber,
Geschäftsführer und Vorstände

Wie gut ist Ihr Unternehmen kommunikativ auf Cyberangriffe und unvorhergesehene Krisensituationen vorbereitet?

Fellows & Sparks

Liebe Leserinnen und Leser,

Cyberangriffe sind heute weit mehr als ein IT-Problem – sie sind Chefsache mit persönlicher Haftung. Spätestens mit dem Start von NIS2 rücken Geschäftsführer, Inhaber und Vorstände noch stärker in die Verantwortung, Sorgfaltspflichten nachweisbar zu erfüllen und im Incident rechtssicher zu führen. Versicherer, Gesellschafter und Aufsichtsbehörden fragen bereits im Vorfeld nach belastbaren Continuity- und Krisenplänen – inklusive klarer Kommunikationslinien. Wer hier Lücken hat, geht ein vermeidbares Haftungs- und Reputationsrisiko ein.

Entscheidend ist Ihre Erstreaktion: Binnen Stunden braucht es ein aktives Lagebild, einen arbeitsfähigen Krisenstab und eine abgestimmte One-Voice-Kommunikation an Mitarbeitende, Kunden, Behörden, Medien und weitere Stakeholder. Struktur schlägt Hektik: Standardisierte Checklisten, definierte Rollen, freigegebene Sprachregelungen und ein Ad-hoc-Statement sind die Grundlage, um Tempo zu machen – ohne teure Fehler zu produzieren.
Unser Ansatz folgt bewährter Einsatzlogik aus dem Krisenhandwerk: Überblick schaffen, Risiko bewerten, entscheiden, handeln – und die Kommunikation von Anfang an professionell führen. Das stärkt Vertrauen, verkürzt Krisen, schützt Werte und Reputation. Viele Handlungsoptionen und Inhalte lassen sich vorbereiten, die notwendigen Routinen, sind trainierbar.

Warum jetzt? Weil die Experten knapp werden. Spätestens 2026 werden viele mittelständische Unternehmen ihre Cyber-Resilienz nachschärfen – mit entsprechend hoher Nachfrage nach spezialisierten Ressourcen. Wer heute vorsorgt, sichert sich Verfügbarkeit, verkürzt Reaktionszeiten und reduziert Haftungsrisiken messbar.

Dieses Whitepaper gibt Ihnen eine kompakte Orientierung und eine praxisnahe Selbstprüfung Ihrer operativen Einsatzfähigkeit.

Nehmen Sie sich eine Stunde –
sie kann im Ernstfall entscheidend sein.

Axel Kühn

Managing Partner
Fellows & Sparks GmbH

Fellows & Sparks

Cyberangriffe sind Chefsache – mit handfesten Herausforderungen für die Unternehmensführung

Digitale Bedrohungen haben längst die Vorstandsetage erreicht. Was früher als IT-Problem galt, ist heute ein existenzieller Krisenfall – mit rechtlichen, wirtschaftlichen und persönlichen Folgen für Geschäftsführung und Vorstand.

Ein erfolgreicher Angriff ist kein hypothetisches Szenario mehr, sondern eine reale Management-Herausforderung. Er fordert innerhalb kürzester Zeit Führung, Entscheidungsstärke und Kommunikationsfähigkeit auf höchster Ebene.

In den ersten Stunden entscheidet sich, ob Sie steuern – oder getrieben werden. Was dann zählt, ist Führungsfähigkeit unter Druck: ein sofort arbeitsfähiger Krisenstab, ein aktuelles Lagebild mit priorisierten Maßnahmen sowie eine One-Voice-Kommunikation.

Wer unvorbereitet ist, verliert wertvolle Zeit – und unter Umständen das Vertrauen von Kunden, Partnern, Investoren oder Aufsichtsbehörden. Richtig teuer werden können allerdings Haftungsrisiken, Reputationsschäden und Betriebsunterbrechungen.

Die gute Nachricht: Mit klaren Verantwortlichkeiten, trainierten Abläufen, redundanten Strukturen und vorbereiteten Sprachregelungen lässt sich das Risiko **substanziell senken** – und die eigene Führungsrolle im Krisenfall stärken.

Steigende Frequenz und Professionalisierung der Angriffe

Cyberangriffe nehmen nicht nur zahlenmäßig zu – sie werden intelligenter, schneller und professioneller.
Laut dem Allianz Risk Barometer 2024 zählen Cybervorfälle erneut zur größten globalen Geschäftsbedrohung – noch vor Lieferkettenproblemen oder Naturkatastrophen. 44 % der befragten Unternehmen weltweit sahen 2024 darin ihr größtes unternehmerisches Risiko.

Besonders perfide: Die Angriffe sind zunehmend industrialisiert. Hinter vielen Attacken stehen heute professionell organisierte Gruppen mit klaren Rollen, ausgeklügelter Arbeitsteilung und sogar Kundensupport. “Ransomware-as-a-Service” ist buchstäblich ein Geschäftsmodell geworden.

Hinzu kommt der Einfluss KI-gestützter Tools. Sie ermöglichen es selbst technisch wenig versierten Tätern, hochwirksame Phishing-Kampagnen oder Deepfakes zu erzeugen. Die Angreifer sind schneller und schwerer zu erkennen – das gilt insbesondere für mittelständische Unternehmen, die mit limitierten Ressourcen agieren.

Die Folgen: Wirtschaftlich, reputativ – und juristisch

Ein Cyberangriff betrifft heute nicht mehr nur Server und Netzwerke. Er stellt die **gesamte Organisation infrage:** Prozesse brechen ab, Lieferketten werden unterbrochen, Kundenkommunikation wird unmöglich, sensible Daten werden gestohlen, blockiert oder veröffentlicht.

- **Wirtschaftlich:** Ein erfolgreicher Cyberangriff führt oft zu unmittelbaren Produktionsausfällen, Lieferengpässen oder Umsatzverlusten. Verträge können nicht erfüllt werden, vereinbarte Fristen verstreichen – mit teils empfindlichen Vertragsstrafen als Folge. Hinzu kommen nicht selten hohe Kosten für forensische Analysen, IT-Wiederherstellung, Rechtsberatung oder externe Kommunikation. Auch Lösegeldzahlungen spielen in vielen Fällen eine Rolle – teils begleitet von staatlicher Überwachung der Zahlungsströme.

- **Reputativ:** Noch gravierender als der finanzielle Schaden kann der Verlust von Vertrauen sein. Kunden, Partner, Investoren oder die Öffentlichkeit erwarten eine professionelle, schnelle und transparente Reaktion – vor allem im Umgang mit sensiblen Daten. Bleibt diese aus, entsteht ein Vakuum, das schnell von Spekulationen, Medienberichten oder Social-Media-Kommentaren gefüllt wird. In dieser Dynamik verliert ein Unternehmen rasch die Kontrolle über die eigene Geschichte – und damit über sein Image.

- **Rechtlich:** Ein Cyberangriff löst in vielen Fällen eine Reihe gesetzlicher Pflichten aus – von der DSGVO über das IT-Sicherheitsgesetz bis hin zur aktuellen NIS2-Richtlinie, die den Rahmen für Cybersicherheit in der EU deutlich verschärft. Verstöße gegen Meldepflichten oder unterlassene organisatorische Vorkehrungen können nicht nur zu Bußgeldern führen, sondern auch zu persönlichen Haftungsrisiken für Geschäftsführer und Vorstände. Zugleich prüfen Versicherungen inzwischen genau, ob präventive Standards eingehalten wurden – andernfalls droht im Ernstfall die Leistungsverweigerung.

Vom Risiko zur Verantwortung: Wer vorbereitet ist, bleibt handlungsfähig

Cyberangriffe lassen sich nicht immer verhindern – aber ihre Folgen lassen sich begrenzen. Voraussetzung dafür ist ein professioneller Umgang mit Risiken: technisch, organisatorisch und kommunikativ.

Denn wenn der Ernstfall eintritt, zählt nicht, ob Sie überrascht wurden – sondern, ob Sie vorbereitet waren. Ein Unternehmen, das Krisenszenarien durchdacht, Rollen geklärt und Kommunikationsprozesse eingeübt hat, kann auch unter Druck souverän agieren. Wer hingegen nur auf eine situative Reaktion setzt, verliert schnell die Kontrolle – über die Lage, die Öffentlichkeit und letztlich die eigene Handlungsfähigkeit.

Im nächsten Kapitel zeigen wir, wie eine Organisation aussieht, die diese Verantwortung ernst nimmt – und sich kommunikativ krisenfest aufstellt.

Zielbild: Wie sieht eine kommunikativ krisenfeste Organisation aus?

Cyberangriffe stellen Führungskräfte nicht nur vor technische, sondern vor organisationale und kommunikative Herausforderungen. Wer im Ernstfall souverän agieren will, braucht klare Prozesse, eingespielte Strukturen und ein Team, das weiß, was zu tun ist – nicht erst im Krisenfall, sondern lange im Voraus.

Viele Unternehmen verlassen sich in der Vorbereitung auf Sicherheitsmaßnahmen der IT oder technische Notfallpläne. Doch Kommunikation ist ein genauso kritischer Faktor: Wird sie nicht mitgedacht, entstehen im Ernstfall gefährliche Lücken – nach innen wie nach außen.

Eine kommunikationsstarke Organisation plant voraus, verteilt Verantwortung, schult ihre Schlüsselpersonen und kennt ihre kritischen Kommunikationsschnittstellen. Sie weiß, wer spricht, wo schnell reagiert werden muss – und wie Vertrauen erhalten bleibt.

Kommunikation im Ernstfall: Der wahre Belastungstest

Ein Cyberangriff wird in aller Regel öffentlich – ob durch Pflichtmeldungen, Medienberichte oder betroffene Kunden. In diesem Moment entscheidet nicht nur die IT-Reaktion über den Verlauf der Krise, sondern vor allem die kommunikative Handlungsfähigkeit des Unternehmens.

Wer spricht? Was wird gesagt? Wann, über welchen Kanal, mit welchem Ton? Genau hier scheitern viele Organisationen. Häufig fehlt eine abgestimmte Kommunikationsstrategie, das Führungsteam ist nicht ausreichend gebrieft, externe Partner sind nicht eingebunden – und die ersten Stunden verstreichen ungenutzt. Im schlimmsten Fall wird vorschnell kommuniziert mit Aussagen, die weiteren Schaden verursachen.

Eine effektive Krisenkommunikation braucht nicht nur Pläne, sondern vor allem Vorbereitung, Zuständigkeiten und ein Incident-Response-Team mit eingespielten Abläufen. Denn in den ersten Stunden zählt jede Entscheidung – und jede Sekunde.

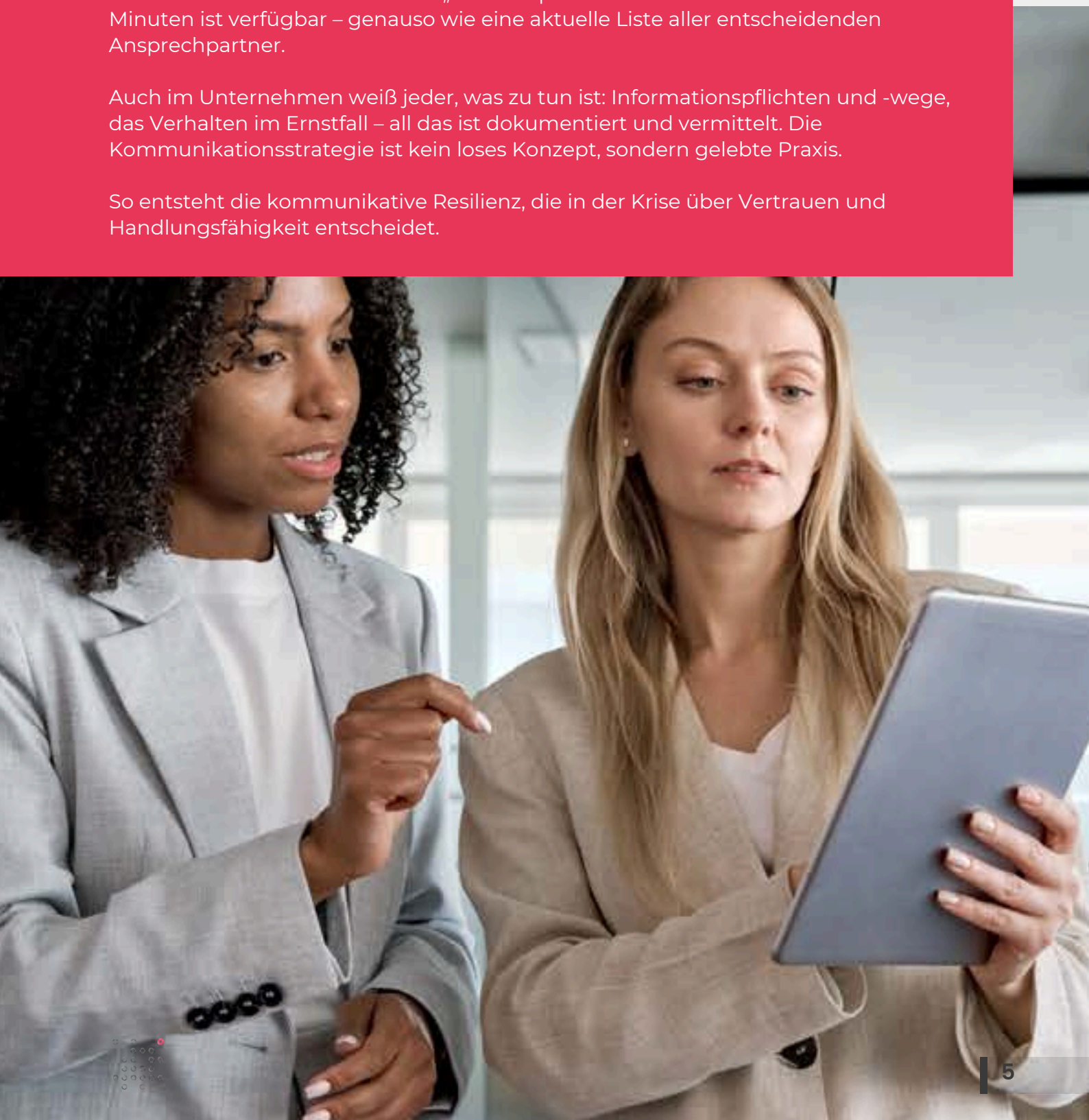
So sieht professionelle Kommunikationsvorsorge aus

In einer gut vorbereiteten Organisation ist Kommunikation Teil der Sicherheitsarchitektur – nicht bloß eine Reaktion auf den Ernstfall. Die Unternehmensführung erkennt ihre Verantwortung: Sie schafft Strukturen, Prozesse und Kompetenzen, um im Krisenfall souverän zu agieren.

Ein eingespielter Krisenstab mit klar definierten Rollen, eingespielten Abstimmungsprozessen, Reaktionsplänen und Entscheidungswegen liegt vor. Die Abläufe wurden erprobt, erste Botschaften vorbereitet, interne und externe Kommunikation strukturiert. Ein „First-Response"-Gerüst für die kritischen ersten Minuten ist verfügbar – genauso wie eine aktuelle Liste aller entscheidenden Ansprechpartner.

Auch im Unternehmen weiß jeder, was zu tun ist: Informationspflichten und -wege, das Verhalten im Ernstfall – all das ist dokumentiert und vermittelt. Die Kommunikationsstrategie ist kein loses Konzept, sondern gelebte Praxis.

So entsteht die kommunikative Resilienz, die in der Krise über Vertrauen und Handlungsfähigkeit entscheidet.



Checkliste: Wie gut ist Ihre Unternehmenskommunikation auf Cyberangriffe vorbereitet?

Cyberangriffe treffen Unternehmen oft ohne Vorwarnung – aber nie ohne Wirkung. Wenn Systeme ausfallen, Daten abfließen oder erste Gerüchte kursieren, ist vor allem eines gefragt: Kommunikationsfähigkeit. Doch die entsteht nicht spontan – sie ist das Ergebnis bewusster Vorbereitung.

Die folgende Checkliste beleuchtet fünf zentrale Aspekte, die über Ihre Resilienz im Ernstfall mitentscheiden: Strategie, Zuständigkeiten, Infrastruktur, Stakeholder-Kommunikation und die Fähigkeit zur Übung und Weiterentwicklung.

Unter jedem Aspekt finden Sie eine Auswahl konkreter Prüffragen.
Alles, was Sie nicht mit einem klaren „Ja“ beantworten können, markiert eine offene Flanke. Und damit einen potenziellen Risikopunkt – für Ihre Handlungsfähigkeit, Ihre Reputation und im schlimmsten Fall für Ihre persönliche Verantwortung.

Bitte beachten Sie:
Diese Checkliste ist kein Ersatz für ein professionelles Audit durch erfahrene Fachleute. Sie liefert erste Hinweise, wo Handlungsbedarf besteht – aber kein vollständiges Bild der tatsächlichen Krisenfestigkeit Ihrer Organisation.

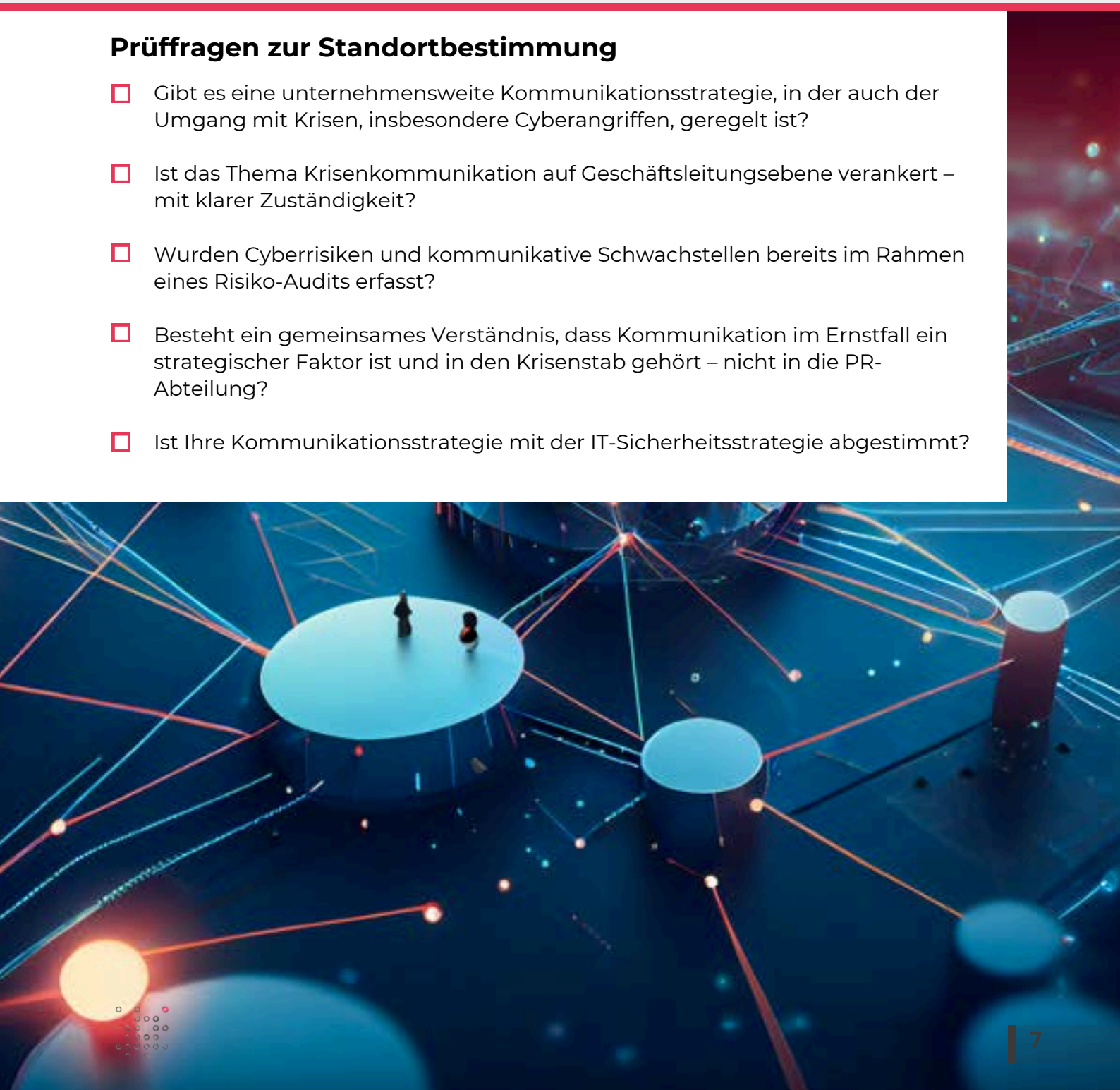
Aspekt 1:
Strategische Verankerung & Risikobewusstsein

Krisenkommunikation beginnt nicht erst im Ernstfall – sie muss strategisch auf C-Level verankert sein. Denn ohne klares Führungsverständnis bleibt Kommunikation reaktiv, fragmentiert und im Zweifel wirkungslos.

Gerade bei Cyberangriffen ist sie ein integraler Teil der Sicherheitsarchitektur – nicht bloß eine Aufgabe für die PR-Abteilung oder externe Agenturen. Fehlt diese Einbindung, geht wertvolle Zeit verloren: Zuständigkeiten sind unklar, Botschaften uneinheitlich, der Reputationsschaden groß.

Prüffragen zur Standortbestimmung

- ☐ Gibt es eine unternehmensweite Kommunikationsstrategie, in der auch der Umgang mit Krisen, insbesondere Cyberangriffen, geregelt ist?
- ☐ Ist das Thema Krisenkommunikation auf Geschäftsleitungsebene verankert – mit klarer Zuständigkeit?
- ☐ Wurden Cyberrisiken und kommunikative Schwachstellen bereits im Rahmen eines Risiko-Audits erfasst?
- ☐ Besteht ein gemeinsames Verständnis, dass Kommunikation im Ernstfall ein strategischer Faktor ist und in den Krisenstab gehört – nicht in die PR-Abteilung?
- ☐ Ist Ihre Kommunikationsstrategie mit der IT-Sicherheitsstrategie abgestimmt?



Aspekt 2:
Rollen, Zuständigkeiten & Krisenteam

Wenn der Ernstfall eintritt, muss klar sein, wer entscheidet, wer zuarbeitet und wer spricht. Ohne einen eingespielten Krisenstab oder ein Incident-Response-Team mit definierten Rollen, klaren Aufgaben und abgestimmten Eskalationswegen entsteht im Krisenfall Chaos statt Kontrolle.

Insbesondere bei Cyberangriffen braucht es ein abgestimmtes Zusammenspiel zwischen Kommunikation, IT, Forensik, Recht und Geschäftsleitung. Nur wenn das Incident-Response-Team auch kommunikativ funktioniert, lassen sich fundamentale Fehler vermeiden.

Prüffragen zur Standortbestimmung

- ☐ Wissen alle im Unternehmen, wen sie ansprechen, wenn eine Cyber-Attacke erfolgt ist oder vermutet wird?
- ☐ Ist definiert, wer die erste Lage erkundet und weitere Entscheidungen trifft?
- ☐ Gibt es einen benannten Krisenstab – und ist dieser auch Pfingstmontag zu erreichen, wenn Ihre IT ausgefallen ist und ihr VoIP-System gehackt wurde?
- ☐ Sind die Mitglieder und speziell die Leiter des Krisenstabs stressresistent und krisenerfahren?
- ☐ Sind alle erforderlichen Kompetenzen am Tisch?
- ☐ Sind Zuständigkeiten und Entscheidungsbefugnisse im Krisenfall eindeutig geregelt und dokumentiert?
- ☐ Ist das Zusammenspiel von Kommunikation, IT und Recht im Ernstfall eingeübt oder zumindest geplant?
- ☐ Existiert ein Kommunikationsleitfaden für Führungskräfte, um in Ausnahmesituationen handlungsfähig zu bleiben?
- ☐ Sind externe Partner (z. B. juristische Beratung, Forensik, Kommunikationsexperten) bereits eingebunden und erreichbar?

Aspekt 3:
Kommunikationsinfrastruktur & operative Handlungsfähigkeit

Im Ernstfall zählt jede Minute – und nichts lähmt ein Unternehmen schneller als der Ausfall der Kommunikationswege. Wer nicht mehr intern oder extern kommunizieren kann, verliert die Kontrolle über die Lage und die Wahrnehmung.

Deshalb braucht es belastbare, auch im Krisenmodus funktionierende Kommunikationsprozesse und Tools: redundant, krisenerprobt, idealerweise unabhängig von der angegriffenen IT-Infrastruktur. Denn auch die beste Strategie nützt nichts, wenn sie in der Stille verpufft.

Prüffragen zur Standortbestimmung

- ☐ Sind Kommunikationskanäle (z. B. Messenger, Mail, Hotline, Intranet) auch bei IT-Ausfällen funktionsfähig?
- ☐ Gibt es Notfalltools oder redundante Systeme für die interne Kommunikation?
- ☐ Existieren dokumentierte Ablaufpläne für verschiedene Krisenszenarien – inklusive Cyberangriff?
- ☐ Liegt ein „First-Response"-Gerüst für die ersten 30 Minuten einer Krise vor?
- ☐ Wurde die operative Handlungsfähigkeit bereits unter Stressbedingungen getestet?

Aspekt 4:
Stakeholder-Kommunikation nach außen & innen

Ein Cyberangriff betrifft nicht nur Systeme – er betrifft Menschen. Kunden, Partner, Behörden und Mitarbeitende erwarten schnelle, klare und vertrauenswürdige Informationen. Wer hier zögert oder widersprüchlich kommuniziert, riskiert nicht nur das Vertrauen, sondern auch rechtliche Konsequenzen.

Deshalb müssen Zeitabläufe, Inhalte und Zuständigkeiten für alle Anspruchsgruppen vorab geklärt sein. Nur so lässt sich sicherstellen, dass im Ernstfall keine Informationslücken und keine Flächenbrände entstehen, wo man Ruhe gebraucht hätte.

Prüffragen zur Standortbestimmung

- ☐ Gibt es vorbereitete Kommunikationspläne für externe Anspruchsgruppen wie Kunden, Medien, Behörden und Partner?
- ☐ Wurden gesetzliche Meldepflichten (z. B. nach DSGVO oder NIS2) identifiziert und in Prozesse überführt?
- ☐ Liegen abgestimmte Botschaften und Sprachregelungen für typische Szenarien vor?
- ☐ Gibt es einen definierten Kommunikationskanal für die Mitarbeitenden – auch im Ausnahmefall?
- ☐ Ist sichergestellt, dass interne Kommunikation Vorrang vor externen Mitteilungen hat (Stichwort: „Betroffene zuerst“)?

Aspekt 5:
Training, Simulation & Partnernetzwerk

Krisenkommunikation funktioniert nur dann, wenn sie regelmäßig trainiert wird. Ein Papier allein macht noch keine Handlungsfähigkeit – was zählt, ist geübte Praxis. Simulationen helfen, Schwachstellen zu erkennen, Rollen zu festigen und Abläufe zu verankern.
Ebenso wichtig: ein eingespieltes Netzwerk aus externen Expertinnen und Experten – von IT-Forensik über Recht bis zur Krisenkommunikation. Nur wenn alle Beteiligten bereits im Vorfeld eingebunden sind, funktioniert die Zusammenarbeit unter Zeitdruck reibungslos.

Prüffragen zur Standortbestimmung

- ☐ Wird die Krisenkommunikation regelmäßig in realitätsnahen Szenarien trainiert?
- ☐ Gibt es dokumentierte Erkenntnisse („Lessons Learned“) aus vergangenen Übungen oder Vorfällen?
- ☐ Werden Führungskräfte gezielt auf kommunikatives Handeln im Krisenfall vorbereitet?
- ☐ Ist ein Netzwerk aus externen Fachleuten (z. B. Recht, Kommunikation, Forensik) aufgebaut – und im Ernstfall erreichbar und einsatzbereit?
- ☐ Wurden Reaktions- und Entscheidungsprozesse mit diesen Partnern bereits abgestimmt und geprobt?

Ihr nächster Schritt:
Von der Erkenntnis zur Handlung

Wenn Sie beim Durchgehen der Checkliste Lücken entdeckt haben oder zentrale Fragen mit „Nein“ beantworten mussten, wissen Sie: Es besteht Handlungsbedarf. Oft reichen schon wenige offene Flanken aus, um die Reaktionsfähigkeit Ihres Unternehmens im Ernstfall massiv zu gefährden – kommunikativ wie organisatorisch.

Hier kommt Fellows & Sparks ins Spiel.

Als erfahrene Spezialisten für **kommunikative Krisenfestigkeit** unterstützen wir mittelständische Unternehmen dabei, sich gezielt auf Cyberangriffe und andere Krisensituationen vorzubereiten. Unser Fokus: die Verbindung von Kommunikationsstrategie, Organisationsentwicklung und operativer Reaktionsfähigkeit.

Die C3-Module:
Unser Baukasten für Ihre Cybersicherheit

Mit unserem **C3-Baukasten** bieten wir ein modulares Unterstützungskonzept, das sich individuell an Ihren Bedarf anpasst – vom schnellen Einstieg bis zur operativen Einsatzbegleitung:

- **C3 Basic-Check - Wissen, wo man steht:** In einem kompakten Workshop analysieren wir gemeinsam mit Ihnen Ihre aktuelle Kommunikations- und Krisenvorsorge. Sie erhalten eine strukturierte Einschätzung sowie konkrete Handlungsempfehlungen zur Weiterentwicklung – inklusive einer „First Aid“-Checkliste. Der ideale Startpunkt für mehr Klarheit und Sicherheit.

- **C3 Professional-Check - Handlungsfähig werden:** Wir vertiefen die Analyse und entwickeln passgenaue Reaktionspläne, Szenarien und Rollenmodelle. Im Anschluss erfolgt ein gezieltes Onboarding Ihrer internen Verantwortungsträger.

- **C3 Response Ready - Handeln können:** Durch gezielte Trainings, Simulationen und Übungen machen wir Ihr Team krisenfest – damit Strukturen nicht nur auf dem Papier bestehen, sondern auch im Ernstfall funktionieren.

- **C3 Response Partners - Unterstützung im Ernstfall:** Wenn es ernst wird, stehen wir an Ihrer Seite – als erfahrene Partner für strategische Kommunikation, Krisenleitung und operative Umsetzung.

Sie möchten eine professionelle Einschätzung darüber, wie gut Ihre Organisation kommunikativ auf Cyberangriffe vorbereitet ist?

Dann ist unser C3 Basic-Check der ideale Einstieg.
Jetzt unverbindliches Vorgespräch vereinbaren: www.fellowsandsparks.com

IHR VERLÄSSLICHER PARTNER FÜR KRISENMANAGEMENT UND CYBERSICHERHEIT

Wer ist die Fellows & Sparks GmbH?

Fellows & Sparks ist eine spezialisierte Unternehmensberatung für strategische Kommunikation und Krisenmanagement mit Sitz in Arnis, Schleswig-Holstein. Seit über 15 Jahren begleiten wir mittelständische und große Unternehmen dabei, ihre Widerstandsfähigkeit in Zeiten tiefgreifender Veränderungen und akuter Bedrohungen zu stärken – insbesondere bei Cyberangriffen.

Ein besonderer Fokus liegt auf der Schnittstelle zwischen technischer Sicherheit und kommunikativer Handlungsfähigkeit. Wir entwickeln maßgeschneiderte Konzepte für Cybersicherheit, Krisenkommunikation und Notfallorganisation – abgestimmt auf Struktur, Branche und Risikoprofil Ihres Unternehmens.

Was uns besonders macht:
Neben unserer eigenen Beratungsexpertise greifen wir auf ein eingespieltes Netzwerk aus Spezialistinnen und Spezialisten zurück – darunter IT-Forensiker, Juristen für Datenschutz und Medienrecht, Kommunikationstrainer, Krisenmanager und technische Fachberater. So können wir im Ernstfall schnell, ganzheitlich und wirkungsvoll unterstützen.

Unser Angebot für Sie:

- **Krisenmanagement:** Aufbau von Notfallplänen, Stabsarbeit, Szenarien und Simulationen
- **Krisenkommunikation:** Entwicklung tragfähiger Kommunikationsstrategien für interne und externe Zielgruppen
- **Prävention & Schulung:** Workshops, Trainings und Awareness-Formate für Mitarbeitende und Führungskräfte
- **Incident Response:** Operative Unterstützung und Koordination im Ernstfall

Warum Kunden uns vertrauen:

- **Interdisziplinäre Tiefe:** Kombination aus Kommunikation, IT-Sicherheit und jurischem Know-how
- **Praxisorientierung:** Lösungen, die im Ernstfall funktionieren – nicht nur auf dem Papier
- **Individuelle Betreuung:** Keine Standardpakete, sondern Strategien, die zu Ihrer Realität passen

Unser Ziel: Ihre Organisation so aufzustellen, dass sie im Krisenfall nicht nur reagiert – sondern handelt. Mit Klarheit, Geschwindigkeit und der richtigen Kommunikation.

Klar. Schnell. Souverän. So erleben Kunden unsere Unterstützung im Ernstfall.

"Das Team von Fellows & Sparks hat uns beeindruckt. Ihre Expertise und die professionelle Arbeitsweise haben uns in einer Krisensituation Sicherheit gegeben. Besonders die Erfahrung im Aufbau und der Führung von Krisenstäben sowie das richtige Priorisieren der vielen Aktivitäten war für uns von unschätzbarem Wert."

Geschäftsführer Maschinenbau, international, 500 Mitarbeitende

„Eine coole Truppe - gerade wenn's brennt. Die wissen, was sie tun."

CEO Sicherheitstechnik, international, 1.300 Mitarbeitende

Liebe Leserin, lieber Leser,

ob ein Unternehmen in der Krise handlungsfähig bleibt, entscheidet sich nicht erst beim Vorfall, sondern in der Vorbereitung: durch klare Zuständigkeiten, abgestimmte Prozesse und eine Führung, die Verantwortung übernimmt.

Dieses Whitepaper liefert erste Orientierung, wo Ihr Unternehmen heute steht – und wo es nachschärfen sollte. Wenn Sie diesen Weg weitergehen möchten, ist unser **C3 Basic-Check** der ideale Einstieg: kompakt, praxisnah und auf Ihre Organisation zugeschnitten.

Lassen Sie uns darüber sprechen, wie gut Ihr Unternehmen kommunikativ wirklich auf den Ernstfall vorbereitet ist.

Jetzt unverbindliches Erstgespräch vereinbaren:
www.fellowsandsparks.com

Ich freue mich darauf, Sie kennenzulernen!

Beste Grüße & bis bald

Axel Kühn
Managing Partner / Fellows and Sparks GmbH

Sie möchten mehr darüber erfahren oder haben andere Fragen zu Ihren Herausforderungen?

Gerne beraten wir Sie in einem persönlichen Gespräch!

+49 4642 924088
mail@fellowsandsparks.com
go-fellowsandsparks.de

Fellows & Sparks