

## Cyberkriminalität / Datensicherheit



Kaum ein Ereignis kann ein Unternehmen so fundamental erschüttern wie eine Cyberattacke. Und doch sind die wenigsten Unternehmen ausreichend auf eine solche Krise vorbereitet. Wenn innerhalb kürzester Zeit kritische Teile der IT-Infrastruktur nicht mehr zur Verfügung stehen, kann die operative Handlungsfähigkeit der Organisation empfindlich eingeschränkt sein. Fallen in einer solchen Lage dann auch noch wichtige Kommunikationskanäle wie E-Mail, Telefon oder das Internet aus, kommt rasch das Gefühl der Ohnmacht hinzu: Denn gerade jetzt verlangen betroffene Stakeholder, vor allem aber Kunden, Lieferanten, Mitarbeiter, Führungskräfte und Behörden, zeitnah belastbare und vertrauensbildende Informationen. Damit wird Kommunikation in der Cyberkrise zu einem erfolgskritischen Faktor.

### WORAUF KOMMT ES AN?

**Haltung zeigen:** Das betroffene Unternehmen muss intern und extern vom ersten Moment an eine klare Position vertreten und konsistent mit einer Stimme sprechen – insbesondere bei Erpressungsversuchen und wenn die Angreifer aktiv die Öffentlichkeit suchen.

**Vorausschauend kommunizieren:** Mögliche Haftungsrisiken von vornherein durch passgenaue Botschaften zum richtigen Zeitpunkt minimieren – nicht zu früh die Rückkehr zur Normalität beschwören.

**Komplexität reduzieren:** Einfache, klare Botschaften und das richtige Timing sind entscheidend. Wer inkonsistent, unverständlich oder zu spät kommuniziert, riskiert Rückfragen der Betroffenen oder der Behörden – und kann Vertrauen beschädigen.

**Mobilisierung und Solidarisierung in einer Ausnahmesituation sicherstellen:** Kommunikation muss in einer Phase hoher Belastung und Unsicherheit den internen Schulterschluss der Belegschaft gegen den Angreifer von außen herbeiführen und aufrechterhalten.

### WAS LEISTEN WIR?

**Beratung in allen Fragen der Kommunikation** sowie erprobtes und belastbares Teamplay mit Rechtsberatern und allen weiteren Funktionen im Krisenstab.

Kurzfristige **Entwicklung aller erforderlichen Kerndokumente** sowie deren zielgruppenspezifische Anpassung für alle relevanten internen und externen Stakeholder.

**Abgestimmte Sprachregelungen** für alle Mitarbeiter mit direktem Kontakt zu Kunden, Lieferanten und anderen Geschäftspartnern.

Frühzeitige Identifikation und Ausarbeitung von **Eskalationsszenarien**, auch vor dem Hintergrund spezifischer Erkenntnisse zur Aufstellung und typischen Vorgehensweise der Angreifer.

Kontinuierliche **Beobachtung und Bewertung der Medienlage** – erforderlichenfalls vertiefende Medienkontaktarbeit und Hintergrundbriefings mit relevanten Redaktionen.

Identifikation **glaubwürdiger Dritter**, die Haltung und Maßnahmen des Unternehmens unterstützen können.

## WORIN BESTEHT DER NUTZEN?

Hohe **Navigationssicherheit und Kontrolle** beim Einsatz von Kommunikation vor dem Hintergrund einer mit hohem Tempo voranschreitenden Ausnahme-situation.

**Minimierung des Haftungsrisikos** und Vermeidung von Bußgeldern und Schadenersatzzahlungen durch passgenaue Botschaften zum richtigen Zeitpunkt in der Kommunikation.

**Vermeidung ressourcenintensiver Rückfragen** durch klare, verständliche Botschaften zum richtigen Zeitpunkt.

**Sicherung des Vertrauens und der Loyalität** kritischer Stakeholder, insbesondere der Mitarbeiter, Kunden und Lieferanten – idealerweise kommt das Unternehmen stärker und geschlossener aus der Krise.

## REFERENZMANDATE:

- Umfassende Beratung und kommunikative Unterstützung eines führenden Lebensmitteleinzelhändlers nach einem massiven Hackerangriff auf die IT-Infrastruktur mit Beeinträchtigung der Lieferfähigkeit und Warenverfügbarkeit in den Filialen. Beratung und Begleitung des Unternehmens durch eine Phase mehrstufiger öffentlicher Eskalation seitens der Angreifer, mit Blick auf konsistente und vorausschauende Kommunikation mit sämtlichen relevanten Stakeholdern.
- Beratung einer Wirtschaftsprüfungsgesellschaft nach einem Hackerangriff auf das Bewerberportal im Internet und dem Verlust personenbezogener Daten. Konzeption und Umsetzung einer proaktiven, entlastenden Medienoffensive vor dem Hintergrund drohender negativer TV-Berichterstattung.
- Beratung eines internationalen mittelständischen Maschinenbau-Unternehmens in der Stakeholder-Kommunikation nach einem Hackerangriff und Datenverlust.
- Beratung und Unterstützung einer Wirtschaftsprüfungsgesellschaft durch umfassende Vorbereitung auf den möglichen Eskalationsfall nach einer frühzeitig aufgedeckten Cyberattacke auf kritische Teile der IT-Infrastruktur in Deutschland.



**Dr. Hartmut Vennen**  
Geschäftsführer

T +49 69 255 388 36  
M +49 160 895 58 58

[hartmut.vennen@vennen-advisors.de](mailto:hartmut.vennen@vennen-advisors.de)

vennen.advisors ist eine unabhängige Managementberatung für Strategische Kommunikation. Wir beraten in Krisen- und Sondersituationen. Als Problemlöser in entscheidenden Momenten schützen und stärken wir Reputation und Geschäftserfolg unserer Mandanten. Dazu nutzen wir unsere jahrzehntelange Erfahrung und Expertise auf dem Gebiet der Strategischen Kommunikation. Darüber hinaus stehen wir Mandanten und ihren Teams in Zeiten des Aufbruchs und der Veränderung zur Seite. Wir sind zuverlässige und engagierte Partner, wenn es darum geht, wichtige Themen und Vorhaben wirksam zu positionieren und damit zum unternehmerischen Erfolg beizutragen.

Durch die bestehende Zusammenarbeit mit dem Team der Strategischen Kommunikationsberatung von FTI Consulting ist es jederzeit möglich, auch solche Mandate realisieren, die ein größeres oder international aufgestelltes Beraterteam erfordern.