# >_Code blue
by Dussmann

## Wer wir sind

Das Serviceportfolio von **Code Blue by Dussmann** umfasst Leistungen zur Absicherung von Organisationen vor, während und nach Cyberkrisen. Das Team besteht aus Experten, die auf Cyber-Risikomanagement, Reputationsmanagement, Datenschutz, Lösegeld-Verhandlungen, Incident Response (IR) und Business Continuity spezialisiert sind.

**Code Blue by Dussmann** ist ein Joint Venture des global agierenden Dienstleistungsunternehmens Dussmann mit Hauptsitz in Berlin und der in Tel Aviv ansässigen Code Blue Ltd. Die Experten von **Code Blue Ltd.** Israel haben bereits zahlreiche komplexe Cyberkrisen erfolgreich bewältigt und die Auswirkungen für ihre internationalen Kunden deutlich minimiert.

Das Dienstleistungsunternehmen **Dussmann** ist Lösungspartner in den Bereichen integriertes Facility Management, Food Services und technischer Anlagenbau. Es ist der größte Geschäftsbereich des Familienunternehmens Dussmann Group, die mit 66.000 Mitarbeitenden in 21 Ländern Dienstleistungen rund um den Menschen bietet.

## 10 Gründe für Code Blue by Dussmann

1. Global Einsatzbereit - Europa, Südamerika, Asien und der Nahe Osten
2. All-in-One-Lösung - Umfassende Bereitschafts- und Krisenmanagementdienste aus einer Hand.
3. Elite-Cyber-Krisenteam - betrieben von Absolventen der Special Forces, die von der U.S. HLS zertifiziert wurden.
4. Cyber Crisis Prediction - Bahnbrechende Vorhersage für Krisenreaktion und Wiederherstellung.
5. Ganzheitliche Risikobewertung - Prüfung von Unternehmensführung, Cyber-Versicherung und finanzieller Widerstandsfähigkeit.
6. Experten für Reputationsmanagement - erfahrene Spezialisten für Kommunikation, Verhandlung und Täuschung.
7. Spitzentechnologie - Technische Plattformen für Bereitschaftsmanagement und Arbeitsplanung.
8. Intelligence-Driven Reputation - Technische Hilfsmittel für fortschrittliches Intelligence- und Reputationsmanagement.
9. Innovativer BCP-Betrieb - Pionierarbeit für den weltweit einzigartigen BCP-Cyber-Betrieb.
10. Maßgeschneidertes Verteidigungsportfolio



# >_ No more crisis!

In einer digalen Welt ist Cybersicherheit nicht verhandelbar

# >_Code blue
by Dussmann

## Cyberkrisenmanagement ist Chefsache

Unternehmensweit stellen Cyberangriffe eine der wenigen Krisensituationen dar, die eine existenzielle Bedrohung darstellen können. Die Lösung von Cyberzwischenfällen darf hierbei nicht allein der IT-Abteilung obliegen, sondern erfordert strategisches Handeln auf Ebene eines Krisenstabs. Dank der umfangreichen Erfahrung in tatsächlichen IT-Notfall- und Krisensituationen verfügen wir über das Know-how, um ein effektives Krisenmanagement zu etablieren. Wir sind in der Lage, Sie im Ernstfall zu unterstützen und eine effektive Kommunikation und Geschäftsfortführung in Krisensituationen zu gewährleisten.

## Krisenmanagement-Team as a Service

Wir wissen, dass ein effektives Cyber-Krisenmanagement idealerweise in die Verantwortung eines zentralen Krisenstabes fallen sollte, der auch für andere Krisensituationen zuständig ist. Dies erfordert einige spezifische Anpassungen.

## Wir bieten folgende Beratungsleistungen:

- Bereitstellung eines Crisis Management-Teams (CMT) und Integration in eventuell bereits bestehende Krisenstäbe.
- Bewertung der Cyber-Risiken, denen Sie ausgesetzt sind oder in Zukunft ausgesetzt sein könnten, sowie Möglichkeiten zur Risikominimierung.
- Zentraler Krisenstab, der notwendige Schnittstellen herstellt und alle zur Krisenbewältigung spezifisch notwendigen Experten aus PR und Reputationsmagement, Incident Response (IR), Datenschutz, Forensik und Verhandlungsführern koordiniert.
- Entwicklung von Cyber-Notfall- und Business Continuity-Plänen nach BSI-200-4 BCM Standard.
- Beratung zum Rollenverständnis und zur Arbeitsweise des Krisenstabes in verschiedenen Szenarien von Cyberangriffen.

www.codebluecyber.de
Code blue GmbH | Stützeläckerweg 14 | 60489 Frankfurt am Main

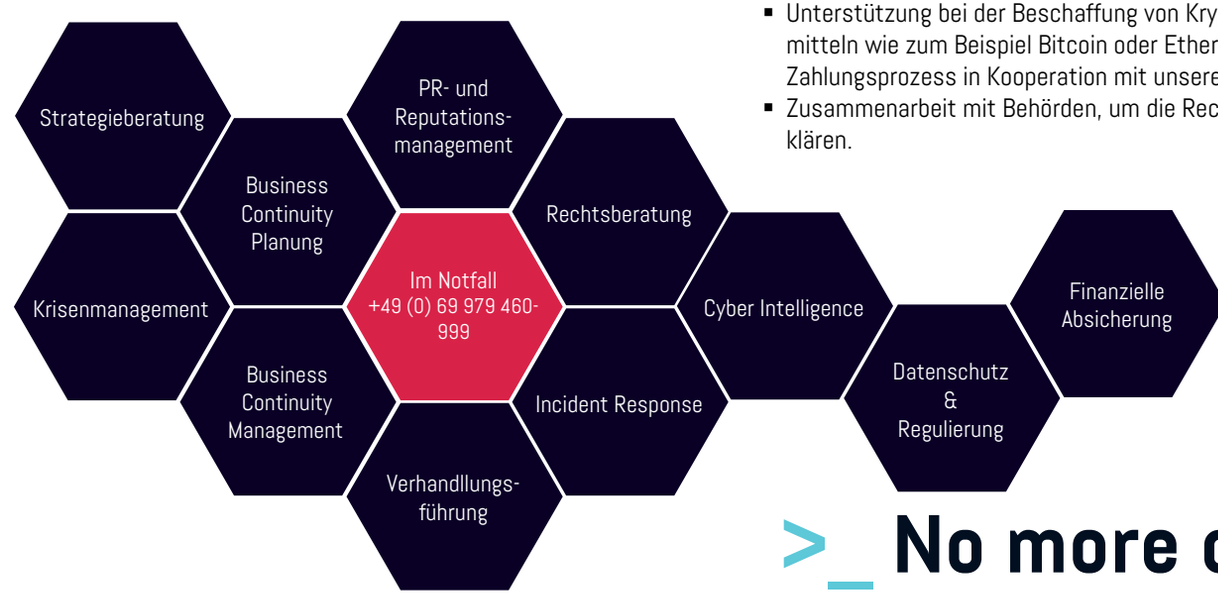
## Cyber-Krisenmanagement Simulationen

In enger Abstimmung mit Ihnen entwickeln wir ein Szenario für eine Simulation des Cyber-Krisenmanagements. Dies kann eine DDoS-Attacke, einen Angriff mit Ransomware oder der Diebstahl von Daten mit anschließender Erpressung umfassen.

Während der Simulation integrieren wir verschiedene Szenarioentwicklungen, moderieren die Krisenmanagement-Simulation und überwachen Ihre Reaktion auf die gespielte Krise in Zusammenarbeit mit unseren Krisenexperten und IT-Experten. Dabei legen wir unseren Fokus auf:

- Ihre Vorgehensweise im Krisenmanagement und den Umgang mit verschiedenen Beteiligten und Stakeholdern.
- Die Art und Weise der Krisenkommunikation.
- Die Aufrechterhaltung der betrieblichen Kontinuität.
- Die Einhaltung von Datenschutzbestimmungen.
- Die von der IT-Abteilung ergriffenen Maßnahmen.

Im Anschluss an die Simulation erhalten sie einen ausführlichen Bericht, in dem wir analysieren, was gut gelaufen ist und wo es Verbesserungspotenzial gibt.




## Schnelle Reaktion bei einem Cybervorfall

Unser Team aus erfahrenen Experten bietet Ihnen einen umfassenden Support als Ihr externes Krisenteam und bildet den Krisenstab in Fällen von Cyberangriffen wie Cybererpressung durch Ransomware, Datendiebstahl und DDoS-Angriffe.

- Sofortige telefonische Beratung und Zusammenstellung eines Krisenstabs innerhalb von vier Stunden bei Ihnen vor Ort oder Remote.
- Fachkundige Betreuung und Beratung durch den Krisenstab.
- Unterstützung bei der Krisenkommunikation, damit Sie die Kontrolle behalten und vor die Lage kommen.
- Wiederherstellung der betrieblichen Kontinuität, um den Schaden zu minimieren.
- Zugang zu Rechtsexperten aus unserem Netzwerk in allen relevanten rechtlichen Fragen.
- Nutzung von aktuellen Cyber Threat Intelligence Informationen zur besseren Entscheidungsfindung.
- Gezielte Recherchen im Darknet, um die Lage einzuschätzen.
- Verhandlung mit Cybererpressern.
- Unterstützung bei der Beschaffung von Krypto-Zahlungsmitteln wie zum Beispiel Bitcoin oder Ether und dem Zahlungsprozess in Kooperation mit unseren Partnern.
- Zusammenarbeit mit Behörden, um die Rechtslage zu klären.

**>_ No more crisis!**