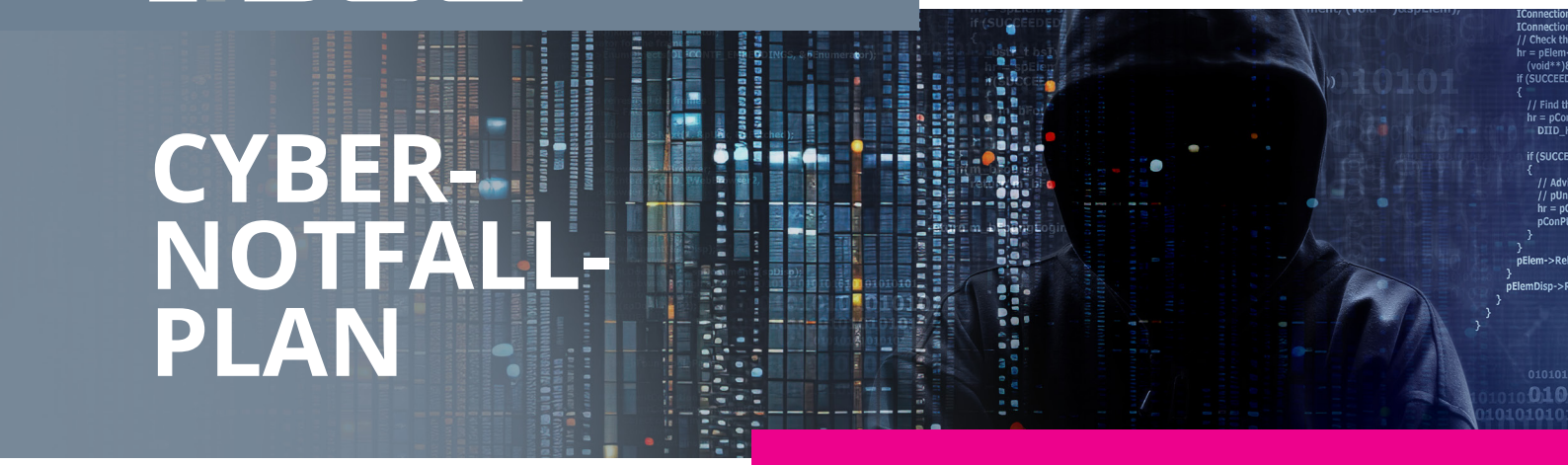
CYBER-NOTFALL-PLAN



SCHADEN HOTLINE
+49 800 181-7237

Cyber-Vorfall?
Wir sind für Sie da!

Was müssen Sie tun?

24/7

Meldung im Schadenfall

Melden Sie den Schadenfall bitte unmittelbar bei der DGC-Schadenhotline (24/7)

Deutschland +49 800 181-7237
International +49 89 21093334
schadenmeldung@dgc.org

Bitte unterlassen

- Keine Unterbrechung der Stromversorgung der IT-Systeme
- Keine Löschung der betroffenen Dateien
- Keine Veränderungen an den betroffenen Systemen durchführen
- Keine Installation der Back-Ups vor einer durch uns beauftragten IT-forensischen Untersuchung.

Erste Schritte im Schadenfall
(am Beispiel einer Ransomwareattacke)

Wie geht es nach der Schadenmeldung weiter?

1. Wir stellen Ihnen umgehend einen Krisenstab aus Experten zusammen.
2. Sofern erforderlich, werden Sie von einem unserer Krisenmanager direkt vor Ort betreut und unterstützt.
3. Gemeinsam analysieren wir den Schaden und stimmen uns zum weiteren Vorgehen gemeinsam ab:
   - » Identifikation erforderlicher Sofortmaßnahmen
   - » Erstellung eines Maßnahmenplans
   - » Einsatz und Koordination des Experten-Teams
   - » Vereinbarung der nächsten Schritte
4. Wir organisieren tägliche Technik- und Management-Besprechungen und stellen so einen strukturierten Austausch zum Status und zu den nächsten Schritten sicher.

Start der Meldekette

Melden Sie den Vorfall bei:

1. Vorstand /Geschäftsführung ☐
2. Leitung der Fachbereiche ☐
   - » IT..... ☐
   - » Finanzen ..... ☐
   - » Recht..... ☐
   - » Compliance..... ☐
3. Datenschutzbeauftragten ☐
4. Risiko-Management ☐
5. Kriminalpolizei ☐

Erste Schritte im Schadenfall
(am Beispiel einer Ransomwareattacke)

Welche Informationen/Daten sollten Sie (nach Möglichkeit) schon für uns und unseren Krisenstab bereithalten?

1. Anzahl der betroffenen Server und Clients
2. Übersicht der Serversysteme: Servername, IP-Adresse, Betriebssystem, Rollen und Dienste (jeweils inkl. Zweck in Kurzform und Kennzeichnung, ob das System aus dem Internet erreichbar ist)
3. Eine Aufstellung über die Netzwerkinfrastruktur (z. B. Netzplan, Netzwerktopologie)
4. Chronologische Auflistung der Auffälligkeiten inkl. der Logs bzw. Mitteilungen der Antibedrohungssysteme
5. Informationen zu den bereits ergriffenen Maßnahmen
6. Informationen über die bisherige Kommunikation – wer wurde bereits informiert?
7. Informationen über die Back-up-Situation – was liegt vor?
8. Informationen zur Hardware vor Ort – was liegt vor?
9. Kontaktliste /Meldekette: Vorstand /Geschäftsführung, Leitung der Fachbereiche (IT, Finance, Recht, Compliance), Datenschutzbeauftragter, IT-Verantwortlicher, Risk-Management, Kriminalpolizei
10. Polizeiliches Aktenzeichen, inkl. des zuständigen Ansprechpartners
11. Interner Krisen-/Notfallplan