

Sehr geehrte Dame, sehr geehrter Herr,

ohne die **Kriminalitätslage** in Deutschland dramatisieren zu wollen, ist festzustellen, dass Sabotageakte, Diebstähle oder Sachbeschädigungen an/von Unternehmenseinrichtungen sowie Wirtschaftsspionage und Konkurrenzausspähung an der Tagesordnung sind.

Auch Hacker-Angriffe auf das Internet und das Abgreifen sensibler Firmendaten haben nach Erkenntnissen der Polizei dramatisch zugenommen.

Bedenken Sie:

Sämtliche Kriminalitätsformen sind mit erheblichen wirtschaftlichen Einbußen sowie Imageschäden verbunden.

Vor diesem Hintergrund bieten wir Ihnen nachfolgend eine Checkliste, mit der Sie selbstkritisch das Notfall- und Krisenmanagement Ihres Unternehmens auf Wirksamkeit prüfen sowie bei Schutz- und Sicherungseinrichtungen ggf. nachbessern können.

Nehmen Sie sich einen Augenblick Zeit!

Vorbemerkung:

Es empfiehlt sich, permanent eine aktuelle Bewertung denkbarer Risiken vorzunehmen und planmäßig besonders gefährliche Szenarien (z.B. Ausfall der IT, Brände, Sachbeschädigungen von erheblichem Ausmaß, Sabotage, Bombendrohungen, Auffinden unbekannter Spreng- und Brandvorrichtungen, Produkterpressung etc.) durchzuspielen.

Die sich daraus ergebenden Konsequenzen sollten festgelegt, Schwachstellen beseitigt werden.

!! Achtung – Straftäter bereiten ihre Aktionen sorgfältig vor!!

Sie . . .

- spähen Objekte aus – von innen und von außen
- checken Zugangssysteme
- bedienen sich der Hilfe von Firmenmitarbeitern und/oder Zulieferfirmen

.../2

Haben Sie optimale Sicherheitsstandards?

Überprüfen Sie Ihre(n)

- Internetauftritt (Skizzen, Lagepläne, Webcams, Luftaufnahmen etc.)
- IT-Sicherungssysteme
- Post-, Paket-, Warenanlieferung
- Mechanische / elektronische Sicherungseinrichtungen
- Firmenparkplätze (Überschaubarkeit, Einwirkungsmöglichkeiten auf Firmenfahrzeuge, Beleuchtungseinrichtungen, Kontrolltätigkeiten)
- Beauftragten Zuliefer- und Fremdfirmen (z.B. Ware Zusteller oder Reinigungsfirmen)

Denken Sie an . . . !

- Ein- und Auslasskontrollen
- Weitere, bisher nicht beachtete Zugangsmöglichkeiten
- Unregelmäßige Kontrollgänge (während und außerhalb der Geschäftszeiten)
- Plausibilitätsprüfungen
- Sensibilisierung von Werkschutz, Pforte/Rezeption und sonstiger Mitarbeiter in Empfangsbereichen
- Festlegung klarer Informations- und Kommunikationswege (die auch in Extremsituationen oder „Chaoslagen“ greifen)
- Betriebsinterne Vorbereitung bei Anschlagsdrohungen (z.B. Bomben- oder Giftanschlägen, Produktmanipulation)

Achten Sie auf . . . !

- Abweichungen vom Alltäglichen
- Personen mit verdächtigem Verhalten
- „Herrenlose“, verdächtige Gegenstände/Taschen/Behältnisse
- Manipulationen an Firmenfahrzeuge
- Sachgerechte Aktenentsorgung / Datenvernichtung
- Fragwürdige Personalfuktuation bei Fremdfirmen

!! Bedenken Sie!! In der täglichen Routine lauert Gefahr!!

.../3

Nachfolgende Fragen sollen Anregung und Denkanstoß zugleich sein:

- 1) Wurden unter dem Eindruck eines **Schadensfalles** in Ihrem Unternehmen (s. Vorbemerkung) **Konsequenzen** gezogen und das Notfall- und Krisenmanagement auf Wirksamkeit überprüft?

ja nein

- 2) Gibt es festgelegte, in einem **Ablaufkalender** erfasste organisatorische Grundsatzentscheidungen für entsprechende **Reaktionen** im Unternehmen bei Eintritt besonders schwerwiegender Ereignisse?

ja nein

- 3) Sind die für die Bewältigung eines Not-, Krisen- oder Schadensfall (nachfolgend Notfall genannt) **erforderlichen Maßnahmen** kalendermäßig erfasst, Verantwortliche bestimmt, Meldewege festgelegt und interne Sicherheitskräfte beteiligt worden?

ja nein

- 4) Sind die **Notfallpläne** oder Maßnahmen bei Eintritt eines Schadens in Ihrem Unternehmen aktuell, inhaltlich aufeinander abgestimmt und zuständigen **Stellen/Entscheidungsträgern** betriebsintern **bekannt**?

ja nein

- 5) Sind **Notfallpläne** in Krisensituationen den Verantwortungs-/Entscheidungsträgern **zugänglich**?

ja nein

.../4

6) Sind **Notfallpläne** und die erforderlichen Maßnahmen ggf. mit zuständigen externen Stellen (z.B. Polizei, Feuerwehr, Rettungsdienste, privater Sicherheitsdienst) **abgestimmt**?

ja nein

7) Haben Sie die im Notfall wichtigen **Meldewege/Erreichbarkeiten** nach Dringlichkeit und Priorität **festgelegt**?

ja nein

8) Haben Sie für den Notfall ein geregeltes Verfahren im **Umgang mit den Medien** festgelegt, (geschulte) Presse-/Mediensprecher namhaft gemacht und für Auskünfte autorisiert?

ja nein

9) Wurde bereits einmal eine Notfallsituation erprobt und sind **Alarmierungsübungen** durchgeführt worden?

ja nein

10) Sind Ihre **Mitarbeiter/Mitarbeiterinnen** auf Notfall- und Krisensituationen **vorbereitet** und angemessen beschult worden?

ja nein

Wichtig:

Da sich Unternehmen ständig weiterentwickeln, Neuerungen und personellen Veränderungen unterworfen sind, sollten Notfallpläne „gepflegt“ und aktuell gehalten werden!!!