Bild-Quelle : Rainer Sturm www.pixelio.de

DATENSCHUTZ REGELBETRIEB

RISIKOIDENTIFIZIERUNG

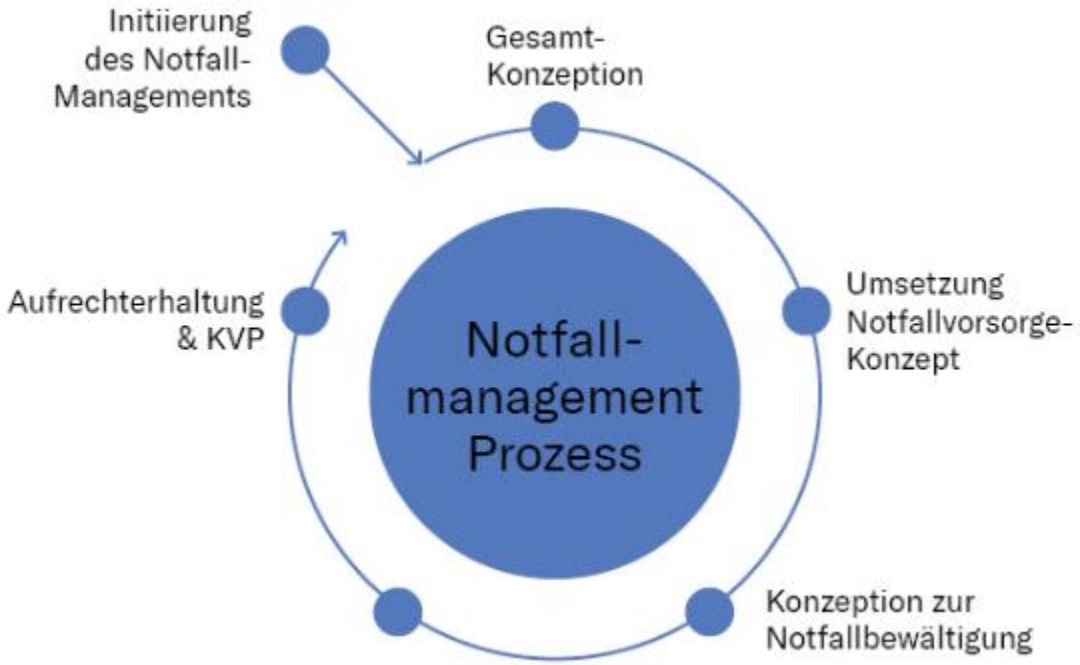

Bild-Quelle : Rainer Sturm www.pixelio.de

Dipl.-Ing Hans-Detlef Krebs

- GF Krebs Consulting & IT-Services (seit 1989)
- GF EuroExpertise (seit 2010)
- Externer Datenschutzbeauftragter seit 2001
- DIN EN ISO/IEC 17024 zertifizierter DSB seit 2010
- Öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung

HD.Krebs@EuroExpertise.eu
HD.Krebs@Krebs-Consulting.de

Bild-Quelle : Rainer Sturm www.pixelio.de

[Interdisziplinärer Ansatz]

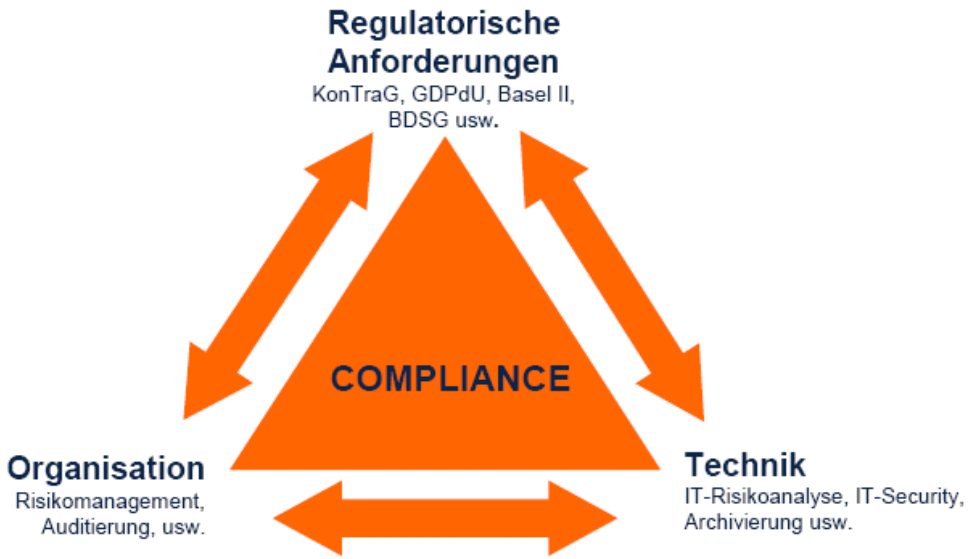

Bild-Quelle : Rainer Sturm www.pixelio.de

Themen heute

Risikoidentifizierung und Handling - Notfallmanagement

- Risikoidentifikation in 5 Schritten
- Prüfpunkte der Unternehmensbereiche und Ihrer Risiken
- Prüfpunkte Notfallmanagement für Unternehmen

Bild-Quelle : Rainer Sturm www.pixelio.de

DATENSCHUTZ

VORWORT

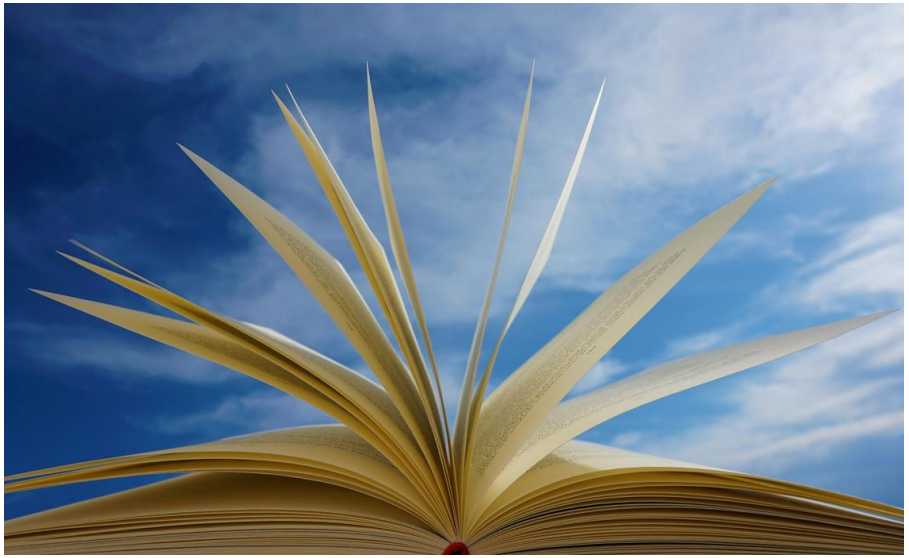

Bild-Quelle : Rainer Sturm www.pixelio.de

Vorwort

- Egal ob Corona-Pandemie, Chipkrise oder Ukraine-Krieg, viele Unternehmen stehen aktuell vor schwierigen Herausforderungen.
- Einerseits muss das Geschäft weiterlaufen, andererseits nimmt die Gefahr zu, etwa auch Ziel von Hackerangriffen zu werden.
- Und vieles hat in diesen Zeiten Datenschutzrelevanz. Auch hier können Schäden drohen.

Besser ist es also, Risiken zu kennen und daran zu arbeiten.

Bild-Quelle : Rainer Sturm www.pixelio.de

Vorwort

- Vielleicht fragen Sie sich zunächst, was Risikomanagement mit uns und unseren Aufgaben als Datenschutzbeauftragter zu tun hat.
- Risiken spielen eine zentrale Rolle. So finden Sie als prägendes Element der Datenschutz Grundverordnung (DSGVO) den **risikobasierten Ansatz.**
- Die Idee dahinter: Es soll im Datenschutz nicht immer das „volle Programm“ durchgezogen werden müssen.
- **Vielmehr sollen Sie Aktivitäten und Maßnahmen passgenau auf die konkrete Verarbeitungssituation zuschneiden**.

Bild-Quelle : Rainer Sturm www.pixelio.de

Vorwort

- Den **risikobasierten Ansatz** finden Sie beispielsweise in **Art. 24 DSGVO**.
- Dieser legt fest, dass Unternehmen zur Umsetzung der DSGVO **geeignete technische und organisatorische Maßnahme**n ergreifen müssen.
- Diese Maßnahmen müssen die **Risiken für die Rechte und Freiheiten natürlicher Personen** im Hinblick auf deren **Eintrittswahrscheinlichkeit und Schwere** berücksichtigen.

Bild-Quelle : Rainer Sturm www.pixelio.de

Vorwort

- Ein weiteres Beispiel sind die Vorgaben zur Sicherheit der Datenverarbeitung (Art. 32 DSGVO).
- Auch hier müssen Risiken erkannt bzw. bewertet und in der Folge mit geeigneten Aktivitäten und Maßnahmen behandelt werden

Bild-Quelle : Rainer Sturm www.pixelio.de

Vorwort

Auch Sie arbeiten risikoorientiert

- Der risikobasierte Ansatz trifft aber nicht nur das Unternehmen.
- Auch wir als Datenschutzbeauftragte sollen uns daran orientieren, wie ein Blick in die DSGVO zeigt.
- So fordert **Art. 39 Abs. 2 DSGVO**, dass Sie bei der Erfüllung Ihrer Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung tragen, wobei Sie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen.
- Diese Risikoorientierung ist besonders wichtig, wenn wir nur über begrenzte (zeitliche) Kapazitäten verfügen.

Bild-Quelle : Rainer Sturm www.pixelio.de

DATENSCHUTZ

Schritte zum Risikomanagement

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 1: Gefahren ausmachen

- Zunächst sollten Sie ein **Brainstorming** bezüglich der möglichen Gefahren für Ihr Unternehmen durchführen, um auszumachen, **welche Ereignisse, Handlungen oder Situationen zu Schäden für Ihr Unternehmen** führen können.
- Wichtig dabei ist, dass Sie **in erster Linie den Fokus auf Datenschutzrelevantes** haben.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 1: Gefahren ausmachen

- Dennoch sollten Sie Gefahren außerhalb des Datenschutzes nie als „irrelevant“ abtun.
- Nicht selten können auch Gefahren in anderen Bereichen, z. B. nicht aktuelle „Bürosoftware“, zum Problem für den Datenschutz werden.
- Gelingt etwa der Hackerangriff, weil Sicherheitslücken ausgenutzt werden konnten, nehmen Kriminelle alles mit. Sie beschränken sich nicht auf die Entwicklungsdaten und machen keinen Bogen um personenbezogene Daten.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 1: Gefahren ausmachen

Brainstorming:

Bei einem Brainstorming gehen Sie folgendermaßen vor:

- Sie machen zunächst das übergreifende Thema aus, das Sie gedanklich angehen wollen. So z. B. „Risiken für den Datenschutz“ oder Datenschutzrisiken durch Auswirkungen des Ukraine-Kriegs“.
- Sie überlegen sich Fragen zum Thema, die Ihre Gedanken sprudeln lassen. Dabei ist klar, je konkreter die Frage ist, desto spezifischer sind die Einfälle.
- Nehmen Sie sich ein großes Blatt Papier oder stellen Sie sich an ein Whiteboard. Notieren Sie kurz die Fragen oder fassen Sie diese in Stichwörtern zusammen und legen Sie dann los. Schreiben Sie alles auf, was Ihnen als Gefahr in den Sinn kommt, sprich alles, was zu einem Schaden für Ihr Unternehmen führen kann.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 1: Gefahren ausmachen

Brainstorming:

Bei einem Brainstorming gehen Sie folgendermaßen vor:

- Schauen Sie sich Ihr „Gemälde“ aus etwas Abstand an und **bewerten Sie Ihre Einfälle**.
- Hier können Sie nun hervorheben, was aus **Ihrer Sicht besonders relevante Gefahren** sind.
- Alles, was eher irrelevant ist, streichen Sie durch.
- Wischen oder radieren Sie nichts weg, vielleicht ändert sich Ihre Einschätzung, wenn Sie die Gefahren beispielsweise mit Kollegen aus dem Unternehmen besprechen

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 2: Geben Sie dem Risiko eine Zahl

- Haben Sie eine Gefahr ausgemacht, ist das noch nicht automatisch ein relevantes Risiko. Hier ist eine Einordnung erforderlich.

Dazu sollten Sie sich an einer einfachen Faustformel orientieren:

- **Die Wahrscheinlichkeit, dass sich die Gefahr realisiert, wird mit der wahrscheinlichen Schadenshöhe multipliziert**. Das ist dann das Risiko für die betreffende Gefahr.

Standardisieren Sie die Bewertung

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 2: Geben Sie dem Risiko eine Zahl

Damit Sie eine gewisse Vergleichbarkeit erreichen und später auch z. B. eine Top-10-Liste der Risiken erstellen können, sollten Sie die Aspekte Eintrittswahrscheinlichkeit und Schadenshöhe standardisieren.

Für die Eintrittswahrscheinlichkeit können Sie festlegen:

Wert Einstufung Maßstab

- 1 **niedrig** einmal oder innerhalb von 5 Jahren
- 2 **mittel** mehrmals oder innerhalb von 2 Jahren
- 3 **hoch** häufig oder kurzfristig

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 2: Geben Sie dem Risiko eine Zahl

Für die Schadenshöhe können Sie eine ähnliche Festlegung treffen:

Wert Einstufung Maßstab

- 1 **niedrig** Geringe finanzielle Schäden sind zu erwarten.
- 2 **mittel** Finanzielle Schäden sind schmerzhaft, aber zu stemmen.
- 3 **hoch** Schäden können existenzbedrohend sein.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 2: Geben Sie dem Risiko eine Zahl

Nicht alle Daten haben gleichen Schutzbedarf

Ihr Fokus liegt grundsätzlich auf dem Datenschutz, sprich auf personenbezogenen Informationen.

Auch die Schutzwürdigkeit von Informationen lässt sich bewerten:

Wert Einstufung Beispiele

1 **niedrig** Rufnummern, E-Mail-Adressen, Kfz-Kennzeichen

2 **mittel** Gehaltsabrechnungen, Steuerbescheide, Zahlungsinformationen von Kunden

3 **hoch** Gesundheitsinformationen, Profile, Kreditinformationen

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 2: Geben Sie dem Risiko eine Zahl

Sprechen Sie mit den Risikomanagern

- So können Sie in Erfahrung bringen, welche Systematik in Ihrem Unternehmen vorgenommen wird.
- Unter Umständen gibt es weitere Aspekte, die einfließen, etwa Auswirkungen auf den Geschäftsbetrieb bzw. die Produktion oder die Lieferfähigkeit.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 3: Überlegen Sie, wie Ihr Unternehmen mit den Risiken umgehen sollte

- Risiken aufzudecken und richtig einzuschätzen ist eine Sache. Eine andere ist, **angemessen auf Risiken zu reagieren**.
- Als Datenschutzbeauftragter ist es Ihre Aufgabe, auf Basis Ihres Fachwissens zu beraten und bei der Entscheidungsfindung zu unterstützen.
- Machen Sie sich Gedanken, welche **Formen der Risikobehandlung** denkbar und passend sind.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 3: Überlegen Sie, wie Ihr Unternehmen mit den Risiken umgehen sollte

Grundsätzlich gibt es folgende Möglichkeiten, mit einem Risiko umzugehen:

- **Risiko minimieren**: Mit wirksamen Gegenmaßnahmen lassen sich Risiken reduzieren.
- **Risiko akzeptieren**: Wenn sich das Risiko nicht mit verhältnismäßigem Aufwand (weiter) reduzieren lässt, muss unter Umständen das Risiko (von der Unternehmensleitung) in Kauf genommen werden.

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 3: Überlegen Sie, wie Ihr Unternehmen mit den Risiken umgehen sollte

- **Risiko übertragen**: Möglicherweise kann Ihr Unternehmen das Risiko auf eine Versicherung übertragen. In der Praxis scheidet diese Möglichkeit jedoch meist aus. Hier gibt es viele Haken und Ösen bzw. es wird schnell ziemlich teuer.
- **Risiko vorbeugen:** Kommt es nicht zur Verarbeitung oder wird diese anders ausgestaltet, entsteht ein Risiko ggf. gar nicht erst

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 4: Unterstützen Sie bei der Entscheidungsfindung

- Eine Gegenmaßnahme reicht oft nicht aus.
- Außerdem können **viele kleine Gegenmaßnahmen** in der Gesamtheit viel **effektiver** sein.
- Lassen Sie diese Aspekte etwa dann einfließen, wenn Sie mit der Unternehmensleitung diskutieren, wie Sie mit den Risiken umgehen sollten

Bild-Quelle : Rainer Sturm www.pixelio.de

Schritt 5: Überprüfen Sie Ihre Einschätzung fortlaufend

- Sind Gefahren und die daraus resultierenden Risiken erfasst, Maßnahmen abgeleitet und umgesetzt, dürfen Sie die Sache nicht einfach beiseitelegen.
- Es sollte **regelmäßig geprüft werden**, **ob die Einschätzungen und Maßnahmen noch passen**.

Bild-Quelle : Rainer Sturm www.pixelio.de

DATENSCHUTZ

Notfallmanagement

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 1: Definieren Sie die Zielgruppen

Unternehmen ist gut beraten, wenn es sich auf **Risiken, Krisen oder Angriffe durch Cyberkriminelle** vorbereitet.

Vielen Unternehmen ist klar:

Der Tag X wird kommen, an dem ein echtes Problem auftaucht.

Umso wichtiger ist, dass man sich gut vorbereitet.

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 1: Definieren Sie die Zielgruppen

Vorbereitung aufs Schlimmste muss einfach sein.

- Als Datenschutzbeauftragter müssen Sie sich um den Schutz personenbezogener Daten kümmern (vgl. Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO)).
- Das heißt vor allem, dass Sie in erster Linie das Unternehmen und die Beschäftigten in Fragen des Datenschutzes beraten.
- Außerdem kontrollieren Sie die Umsetzung der gesetzlichen oder betrieblichen Festlegungen zum Datenschutz.

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 1: Definieren Sie die Zielgruppen

Vorbereitung aufs Schlimmste muss einfach sein.

- Dazu zählt etwa auch, dass die Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DSGVO gewährleistet ist.
- So müssen insbesondere technische und organisatorische Maßnahmen passen und funktionieren, damit personenbezogene Daten etwa vor Vernichtung und Verlust geschützt sind.
- Hier kommt es darauf an, dass die **Maßnahmen risikoangemessen** sind (Art. 32 Abs. 2 DSGVO)

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 2:

Verdeutlichen Sie, dass es nicht nur um personenbezogene Daten geht

Unter Umständen müssen Sie auch das Management überzeugen.

- Sich gut auf Notfälle oder Worst-Case Szenarien vorbereiten ist nicht nur für den Datenschutz relevant.
- Vielmehr sind datenschutzrelevante Szenarien, etwa ein Hackerangriff oder die Zerstörung des Serverraums bei Hochwasser, nur ein Teil des Risikouniversums.
- Wie inzwischen jeder weiß, können auch Lieferengpässe, Kriege oder Krisen dazu führen, dass Systeme nicht mehr genutzt werden können oder Produkte und Services nicht mehr zur Verfügung stehen.
- Dadurch kann Ihr Unternehmen große Probleme bekommen, etwa wenn es um die eigenen angebotenen Produkte und Services geht.

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 2:

Verdeutlichen Sie, dass es nicht nur um personenbezogene Daten geht

Um Ihr Gegenüber außerhalb des Datenschutzes von der Sinnhaftigkeit von Notfallvorsorgemaßnahmen zu überzeugen, helfen Ihnen zusätzlich folgende Argumente:

- Daten sind der Schatz des Unternehmens: Wenn Ihr Hinweis auf die Notwendigkeit einer Notfallplanung als kostspielige Schwarzmalerei abgetan wird, stellen Sie doch einfach mal die Frage, wie lange Ihr Unternehmen wohl auf die Kundendatenbank oder wichtige Projektdaten verzichten kann, ohne dass der Geschäftsbetrieb Schaden nimmt und der Umsatz leidet.

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 2:

Verdeutlichen Sie, dass es nicht nur um personenbezogene Daten geht

Um Ihr Gegenüber außerhalb des Datenschutzes von der Sinnhaftigkeit von Notfallvorsorgemaßnahmen zu überzeugen, helfen Ihnen zusätzlich folgende Argumente:

- Risikomanagement ist ein Muss: Einfach nach Lust und Laune wirtschaften kann heutzutage kein Unternehmen mehr. Man muss Risikovorsorge betreiben.
- Hierauf achten beispielsweise auch Wirtschaftsprüfer.

Bild-Quelle : Rainer Sturm www.pixelio.de

Notfallmanagement Punkt 3:
Prüfen Sie, was wie der Status Quo ist

- Wollen Sie dem Notfallmanagement Ihres Unternehmens einmal prüfen, können Sie ein vorhandenes Konzept als Sollzustand ansehen und den Istzustand bewerten.
- Wollen Sie das Thema grundsätzlich auditieren, können Sie die folgende Checkliste einsetzen

Bild-Quelle : Rainer Sturm www.pixelio.de

Gefahr	Erklärung
Cyberkriminalität	
Erfolgreicher Angriff auf das Firmennetzwerk	Sind etwa Hacker erst einmal ins Netzwerk eingedrungen, ist meist nichts mehr vor ihnen sicher. Hier sind Schutzmaßnahmen nötig, etwa um Eindringversuche zu erkennen.
Lahmlegen von Datenbanken und Systemen durch Hacker	Dies kann beispielsweise dazu dienen, Schutzgeld vom Unternehmen zu erpressen. Ziel der Angreifer kann aber auch eine Straf- oder Racheaktion sein.
Verschlüsselung aller wichtigen Daten und Dateiablagen im Unternehmen durch Kriminelle	Hier zielen die Kriminellen oft auf Lösegeld ab. Doch meist verschlüsseln sie die Daten nicht nur, sie greifen sie vorher ab. So lässt sich mindestens zweimal kassieren. Oder die Daten werden anderswo zu Geld gemacht.
Denial-of-Service-Angriff auf Webseite oder Onlineshop	Ist etwa der Onlineshop besonders wichtig, muss sich Ihr Unternehmen davor schüt zen, dass er durch zu viele gleichzeitige Anfragen nicht mehr erreichbar ist. Als Gegen maßnahme müssen hier ggf. Server aufgerüstet und Kapazitäten erhöht werden.
Diebstahl von Accounts und Identitäten	Denken Sie hier an Accounts in Messengern und sozialen Netzwerken. Werden diese gekapert, ist das schnell ein großes Problem.

Bild-Quelle : Rainer Sturm www.pixelio.de

Gefahr	Erklärung
Informationstechnologie	
Ausfall von IT-Systemen, Server oder Netzwerktechnik aufgrund technischen Defekts	Beispielsweise Netzwerktechnik oder Server können kaputtgehen. Dann stellt sich die Frage „Wie geht es nun weiter?“.
Ausfall von Systemen, Technik und Datenbanken aufgrund Stromausfalls	Stromausfälle können große Probleme verursachen. Passieren sie im falschen Moment, kann viel Schaden angerichtet werden.
Diebstahl von Systemkomponenten	Auch das kann passieren. Weil Technik oder Kabel viel Geld bringen, können Lang finger zugreifen, eventuell sogar im gesicherten Serverraum.
Ausfall eines in den IT-Betrieb eingebundenen Dienstleisters	Ein Dienstleister kann pleitegehen oder den Betrieb einstellen. Was macht Ihr Unter nehmen, wenn dieser für das eigene Unternehmen wichtig ist und etwa Systeme, Software oder Daten nicht mehr verfügbar sind?

Bild-Quelle : Rainer Sturm www.pixelio.de

Gefahr	Erklärung
Standort, Gebäude und Büro	
Ausfall von Standorten oder Gebäuden	Es kann viele Gründe geben, warum ein Gebäude nicht mehr betreten werden darf, etwa ein Brand. Dann müssen Alternativen zur Verfügung stehen.
Betreten von Gebäuden und Büros durch Unbefugte	Dieser Aspekt zielt auf die Standortsicherheit ab. Wie schützt man sich vor Einbrechern, Saboteuren & Co.?
Deaktivierung vorhandener Sicherheitstechnik bei fehlender Stromversorgung	Reicht ein Stromausfall aus, damit alle Sicherheitseinrichtungen „tot“ sind, haben Täter leichtes Spiel, gerade nachts oder am Wochenende.

Bild-Quelle : Rainer Sturm www.pixelio.de

Gefahr	Erklärung
Datenschutzrelevantes	
Diebstahl außerhalb der Arbeitszeit	Geraten Daten in falsche Hände, ist Ärger vorprogrammiert. Deshalb braucht es passende Gegenmaßnahmen, etwa Verschluss und Daten-/Geräteverschlüsselung.
Unbefugte Kenntnisnahme von Informationen am Empfang	Am Empfang geht es oft etwas hektischer zu. Unter Umständen kommen Unbefugte an Informationen, die nicht für ihre Augen und Ohren bestimmt sind.

Bild-Quelle : Rainer Sturm www.pixelio.de

DATENSCHUTZ

Checkliste Notfallmanagement

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 1:

Ist ein **Regelwerk** vorhanden, aus dem sich **Zuständigkeiten, Verantwortlichkeiten, Prozesse und Maßnahmen** ergeben?

Hintergrund:

- Generell sollte es eine Rahmenregelung geben, aus der sich Zuständigkeiten, Verantwortlichkeiten und das Vorgehen im Fall der Fälle ergeben.
- Die schriftliche Fixierung und Freigabe durch die Unternehmensleitung sind besonders wichtig, damit es im Fall der Fälle zu keinen Diskussionen oder Verzögerungen kommt.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 2:

Existiert ein **Notfallkonzept** oder **Notfallhandbuch**?

Wenn ja, ist es auf dem aktuellen Stand?

Hintergrund:

- Fehlt ein Notfallkonzept oder -handbuch ganz bzw. ist es nicht mehr auf dem aktuellen Stand, sollten Sie unverzüglich dieses To-do anstoßen.
- Bestehen solche Dokumente, müssen die Inhalte aktuell sein.
- Achten Sie beispielsweise auf Ansprechpartner sowie Telefonnummern und E-Mail-Adressen.
- Sind diese Angaben veraltet, kann es im Fall der Fälle nicht nur zu Verzögerungen kommen.
- Es drohen auch Fehlentscheidungen oder das Ausbleiben von nötigen Entscheidungen, weil nicht klar ist, wer entscheiden darf

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 3:

Ist klar definiert, **bei welchen Ereignissen** von einem **Notfall** gesprochen wird?

Hintergrund:

- Notfall ist nicht gleich Notfall.
- Eventuell kann Ihr Unternehmen auf bestimmte Systeme oder Daten auch länger verzichten.
- Andere können hingegen zum Mega-GAU für das Unternehmen werden, auch wenn sie nur kurzzeitig nicht mehr verfügbar sind.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 4:

Sind mit der Definition wirklich **alle in Betracht kommenden Notfälle** erfasst?

Hintergrund:

- Legen Sie gemeinsam mit Ihren Gesprächspartnern fest, welche Fälle das Unternehmen lahmlegen könnten und dementsprechend als Notfälle zu bezeichnen sind.
- Betrachten Sie aber auch „banale“ Notfälle, wie etwa ein längerer Stromausfall oder die Unbenutzbarkeit von Gebäuden nach einem Löscheinsatz der Feuerwehr.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 5:

Ist konkret beschrieben und festgelegt, **wer befugt ist, notfallspezifische Entscheidungen** zu treffen?

Hintergrund:

- Wichtig ist, dass die Entscheidungsträger kompetent sind, die richtige Entscheidung zu treffen.
- Hierfür muss das notwendige Fachwissen vorhanden oder schnell verfügbar sein.
- Auch hier gilt: Die Informationen über die Ansprechpartner wie beispielsweise Name und Telefonnummer müssen immer auf dem aktuellen Stand gehalten werden.
- Sind die Angaben veraltet, kann in einem Notfall die Suche nach den Zuständigen wertvolle Zeit kosten.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 6:

Haben die zuständigen Personen die erforderlichen Vollmachten und Berechtigungen und sind diese über ihre Aufgaben und Befugnisse informiert?

Hintergrund:

- Eventuell erscheinen Konzepte auf den ersten Blick vollständig, weil etwa Ansprechpartner genannt sind.
- Nötig ist jedoch auch, dass festgelegt ist, welche Entscheidungsbefugnisse die betreffenden Personen haben.
- Auch müssen die Personen von ihrem „Auftrag“ Kenntnis haben.
- Fragen Sie doch einfach mal bei den genannten Personen nach, was diese zu ihrer Aufgabe im Fall der Fälle wissen.
- Ansonsten erstellen Sie eine Liste mit Verantwortlichen und der Beschreibung Ihren Zuständigkeiten

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 7:

Gibt es **Anweisungen, Prozessbeschreibungen oder Checklisten** für bestimmte Szenarien?

Hintergrund:

- In Notfällen wird es meist hektisch. Fehlt jetzt die Orientierung und ist kein genauer Plan vorhanden, wie vorzugehen ist, bricht Panik aus. Dadurch kann sich die Lage noch weiter verschlimmern.
- Um einen kühlen Kopf zu bewahren und falsche oder übereilte Entscheidungen zu vermeiden, sind genaue Arbeitsanweisungen inklusive einer Schritt-für-Schritt-Notfall-Checkliste mit detaillierten Vorgaben Gold wert.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 7:

Gibt es **Anweisungen, Prozessbeschreibungen oder Checklisten** für bestimmte Szenarien?

Prüfen Sie die Checklisten auf diese Aspekte:

- Sind die Handlungsanweisungen eindeutig formuliert (z. B. Anweisungen mit Ja-Nein Entscheidungen)?
- Sind die Anweisungen kurz und leicht verständlich?
- Ist das definierte Vorgehen schlüssig und umsetzbar?

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 8:

Sind für bestimmte Szenarien **Sofort-, Folge- und Eskalationsmaßnahmen** festgelegt?

Hintergrund:

- Es kann sinnvoll sein, sich für bestimmte Szenarien genau zu überlegen, was beim Eintritt des Notfalls sofort zu erledigen ist. Hier können auch banale Aspekte wichtig sein. Bei einem Virenausbruch auf einem Computer z. B. ist es besonders wichtig, dass dieser vom Netzwerk getrennt wird.
- Denken Sie aber auch an den Fall, dass Sofortmaßnahmen nicht funktionieren. Hier hilft es nicht, wenn die Maßnahme immer wieder versucht wird. Hier muss eskaliert werden und etwa auf anderer Ebene entschieden werden, was zu tun ist.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 9:

Existieren **Notfallpläne bezüglich Fortführung der Geschäftstätigkeit**?

Hintergrund:

- Prüfen Sie auch den Aspekt, dass etwa Technik ausfällt oder Daten nicht mehr oder vor- übergehend nicht verfügbar sind.
- Gibt es Planungen dazu, wie die Aktivitäten des Unternehmens (z. B. Vertrieb, Produktion, Logistik) fortgeführt werden können, etwa mit analogen Mitteln?

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 10:

Besteht ein **Kommunikationskonzept**?

Hintergrund:

- Nicht vergessen werden darf, dass informiert werden muss.
- Denken Sie etwa an das Informieren von Beschäftigten oder Geschäftspartnern.
- Hier sollte ebenfalls ein Konzept für den Notfall vorhanden sein.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 11:

Gibt es **für wichtige IT-Systeme bzw. Datenverarbeitungsverfahren**

Konzepte zur Datensicherung (**Back-up-Konzepte**)?

Hintergrund:

- Der „Rettungsanker Nummer eins“ ist oft ein Back-up von Systemen, Betriebssystemen, Software und Daten.
- Im Fall der Fälle können die nötigen Daten aus den Sicherungen wiederhergestellt werden.
- Das kann für die Fortführung oder den Wiederanlauf des Geschäftsbetriebs entscheidend sein.
- Prüfen Sie hier auch: Wo werden die Sicherungen gelagert?
- Sind die Sicherungen etwa für Cyberkriminelle unerreichbar?

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 12:

Sind in den **Konzepten und Szenarien Risiken bei anderen Stellen** berücksichtigt?

Hintergrund:

- Denken Sie hier etwa an den Anbieter von Software- oder Speicherlösungen im Internet bzw. in der Cloud.
- Auch diese können aufgrund einer Krise oder eines Notfalls nicht mehr verfügbar sein?

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 13:

Wurde das **Eintreten von Szenarien oder Notfällen durchgespielt** und wurden die Konzepte getestet?

Hintergrund:

- Ob Notfallvorsorge wirklich etwas bringt und die Planung funktioniert, sollte man im Fall der Fälle testen.
- Einem solchen „Realtest“ sollten Übungen und Tests vorangehen, damit
- man Unzulänglichkeiten und Umsetzungsprobleme erkennt und angehen kann.

Bild-Quelle : Rainer Sturm www.pixelio.de

Frage 14:

Wie wird **überprüft, ob Regelwerke, Konzepte und Umsetzungsmaßnahmen** im Laufe der Zeit **noch passen**?

Hintergrund:

- Ein gutes Konzept muss regelmäßig aktualisiert und angepasst werden.
- Schließlich können sich viele Rahmenbedingungen verändern, die erhebliche Auswirkungen auf das Funktionieren der Konzepte haben können.
- Hinterfragen Sie das Vorgehen bei Aktualisierung und Anpassung aller relevanten Dokumente und Vorgaben.

Bild-Quelle : Rainer Sturm www.pixelio.de

Kontakt:

EuroExpertise GmbH

European IT-Expert and Data Protection

Am Stift 4-6
44263 Dortmund

Telefon +49-0231-222845-0
Telefax +49-0231-2228 49

E-Mail HD.Krebs@EuroExpertise.eu

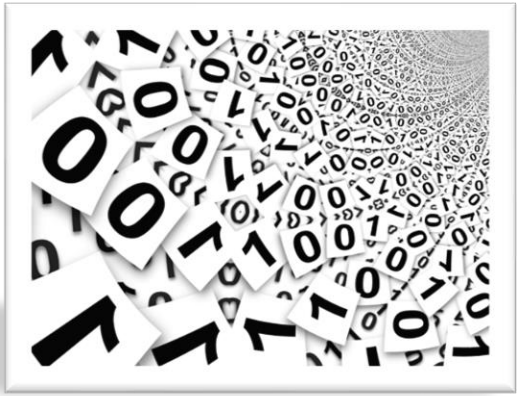

Bild: © Gerd Altman / pixelio.de

Lizenzfreie Bilder verwendet von www.pixelio.de