

IT-Notfallplanung



AGENDA



Einleitung

Warum IT-Notfallplanung

Was ist IT-Notfallplanung

Der IT-Notfallplan

**Es kommt nicht darauf an,
die Zukunft zu wissen,
sondern auf die Zukunft
vorbereitet zu sein**
(Perikles)

Was würde geschehen...



... wenn aus Ihrem Unternehmen personenbezogene oder sensible Unternehmensdaten an die Öffentlichkeit gelangen?

...wenn in Ihrem Unternehmen Datenbestände oder Hardware mutwillig oder durch ein Unglück unwiederbringlich zerstört würden?

... wenn aus Ihrem Unternehmen Massen-E-Mails (Spam) mit Computer-Viren vorsätzlich oder versehentlich verschickt werden?

...wenn über Server Ihres Unternehmens urheberrechtlich geschützte Daten oder anstößige Fotos im Internet getauscht oder verkauft werden?

Welche Konsequenzen können Ihrem Unternehmen und den verantwortlichen Personen drohen?

Typische Mängel bei IT-Sicherheitsüberprüfungen in Unternehmen zeigen schnell wo die Ursachen für Probleme bei der IT-Notfallplanung liegen können...

...mangelhafte, unvollständige oder keine dokumentierte IT-Notfallplanung

...unvollständige oder keine Dokumentation des Netzwerks und der Abläufe

...mangelhafte Brandverhütungsvorsorge

...mangelhafte Datensicherungskonzeption

...mangelhafte organisatorische Absicherungsmaßnahmen der Zugänge zu sensiblen Unternehmensbereichen

...unzureichende Einweisung und Kenntnis der Mitarbeiter über IT-Notfallmaßnahmen

...keine Festlegung der Verantwortlichkeiten für die IT-Notfallvorsorge

...keine Durchführung von IT-Notfallübungen

...unbehelligter Zugang ins Unternehmen für fremde Personen

... nachlässige Regelungen für den Umgang mit mobilen Datenträgern, Smartphones und Notebooks

...man kann fast alles korrigieren und nacharbeiten...

aber:

Verlorene oder zerstörte Daten sind unter Umständen unwiderruflich und für immer verloren!

Durch IT-Ausfall nicht getätigte Geschäfte gehen eventuell verloren!

Image- und Vertrauensverlust kann langfristig zur Beendigung der Zusammenarbeit mit Geschäftspartnern führen!



Notwendigkeit einer IT-Notfallplanung

Das KonTraG ("Gesetz zur Kontrolle und Transparenz im Unternehmensbereich,") sagt hierzu eindeutig (§ 91 Abs. 2 AktG):

"Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Im Klartext bedeutet dies, dass jeder Geschäftsführer bei mangelhafter physikalischer IT-Sicherheit grob fahrlässig handelt und persönlich haftet, wenn dem Unternehmen daraus Schäden zugefügt werden. Bei Kreditinstituten kommt verschärfend der aufsichtsrechtliche Anforderungskatalog hinzu.



Restrisiko

Grundsätzlich können Restrisiken im Sinne der Angemessenheit und Tragbarkeit bestehen bleiben...

...allerdings erwartet der Gesetzgeber, dass diese nachvollziehbar sind und soweit entschärft werden, dass sie den Geschäftsbetrieb im Eintrittsfall nicht maßgeblich gefährden!



Was sind denn eigentliche IT-Notfälle?

Elementarschäden (Katastrophen)...

wie sie z.B. durch Feuer, Wasser, Erdbeben, Blitzeinschlag und sonstige Unwetter eintreten können

aber auch...

Virenbefall, Hackerangriff, Ausfall der Telekommunikationsanlage, Verlust sensibler Datenbestände, nicht autorisierte Weitergabe sensibler Datenbestände, defekte Datensicherung, Ausfall von Festplatten, Verlust von Notebooks mit unverschlüsselten Festplatten, Verlust mobiler, unverschlüsselter Datenträger (z.B. USB-Sticks) Verlust von Smartphones, Diebstahl von Hardware oder Datenbeständen u.v.m.

**Es ist besser, Deiche zu bauen,
als darauf zu hoffen,
dass die Flut allmählich Vernunft
annimmt.**

(Zitat: Hans Kasper, dt. Schriftsteller und Hörspielautor)

Grundlagen für die IT-Notfallplanung

BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4: Notfallmanagement

BSI Grundschutzhandbuch



Bundesamt
für Sicherheit in der
Informationstechnik

IT-Notfallhandbuch Teil A:

Allgemeiner Überblick über die IT-Umgebung.

**Geographische und unternehmensspezifische
Verhältnisse im Bezug auf generelle Vorsichts-
und Vorsorgemaßnahmen.**



IT-Notfallhandbuch Teil B:

Alarmmanagement bei Eintritt eines IT-Notfalls



IT-Notfallhandbuch Teil C:

Gefährdungsanalyse bezogen auf die besonderen Verhältnisse des Serverraums.

Feststellung, welche DV- Abläufe vorrangig wieder aufgenommen werden müssen.



Das IT-Notfallhandbuch...

...enthält Angaben, deren Kenntnis unbefugte Personen dazu verwenden können, Ihrem Unternehmen wesentlichen und nachhaltigen Schaden zuzufügen



Empfehlung für die Vorgehensweise bei der IT-Notfallplanung im Rahmen der Erstellung des IT-Notfallkonzepts

strukturierte Aufnahme der Ist-Situation und der individuellen Anforderungen

Bewertung der Ist-Lage und Identifizierung möglicher Schwachstellen

Empfehlungen für eine rasche und pragmatische Schwachstellenbeseitigung

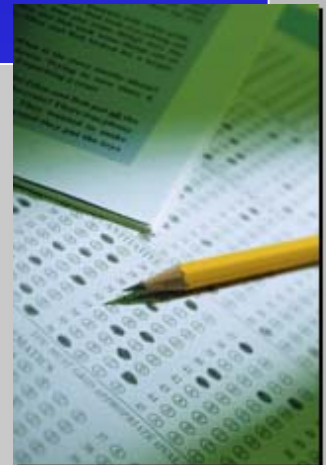
**Wer über kein Notfallkonzept verfügt,
verliert unter Umständen wertvolle Zeit !**

**Ein für den IT-Notfall vorgedachtes, aktuelles und
umfassendes IT-Notfallkonzept hilft im
Falle eines Falles.**

**Katastrophen lassen sich durch eine sinnvolle
IT-Notfallplanung und durch die damit mögliche
rechtzeitige Reaktion auf Notfälle
in ihren Auswirkungen begrenzen oder sogar verhindern.**



Sichere IT-Umgebungen sind kein statischer Zustand, sondern ein ständiger Prozess, der einer regelmäßigen Prüfung und Anpassung unterliegen muss!



Stellen Sie sich daher immer folgende Fragen:

Welche Auswirkungen hat es für mein Unternehmen, wenn wichtige Computer, Daten oder andere IT-Komponenten plötzlich ausfallen und für längere Zeit nicht mehr nutzbar sind?

Kann die tägliche Arbeit noch weiter fortgesetzt werden?

Wie hoch wäre der mögliche Schaden für mein Unternehmen?

Vielen Dank für Ihre Aufmerksamkeit.

Haben Sie noch Fragen

