Best practice	**Datensicherung**
Autor	**Bernd Maierhofer/dato**
Datum	**29.8.2022**
Version	**4**

Dieses Dokument enthält die wichtigsten Punkte, die zum Thema Datensicherung zu beachten sind. Ein Tipp vorneweg: Datensicherung schützt Sie davor, dass Ihre Daten UNWIEDERBRINGLICH verloren sind. Lassen Sie den Begriff „unwiederbringlich“ ein wenig wirken.

Aus der Praxis:

- Der Laptop wird gestohlen/geht kaputt/wird ersetzt.
- Ein Techniker ist übereifrig und löscht beim Update des Betriebssystems die Festplatte.
- Die Studie ist längst fertig, den Rechner gibt es schon lange nicht mehr, da ergibt sich ein Folgeprojekt, das auf den damaligen Daten aufsetzt.

Jeder der folgenden Punkte ist als ToDo einer Checkliste zu verstehen. Es folgt eine Begründung mit weiteren Hinweisen sowie einer kurzen Beschreibung, was passieren könnte, wenn man diesen Punkt nicht umsetzt. Die Reihenfolge der Punkte spiegelt keine Priorität wider.

Die Datensicherung wird durchgeführt und ich kann das leicht überprüfen.

Die Datensicherung wird manuell oder automatisch durchgeführt. Es wurde ein Ort festgelegt, an dem die Datensicherung erzeugt wird. Es wurde festgelegt, welche Daten gesichert werden. Es wurde überprüft, dass die Datensicherung am gewünschten Ort erzeugt wird. Es wurde überprüft, dass die zu sichernden Datenbestände tatsächlich gesichert werden.

Worst Case: Wird die Datensicherung nicht oder nicht vollständig durchgeführt, können Daten unwiederbringlich verloren gehen.

Es sind sinnvolle Intervalle festgelegt.

Die Intervalle, in denen eine Datensicherung erzeugt wird, sind sinnvoll gewählt und auf die Änderungsfrequenz der Daten abgestimmt.

Worst Case: Im schlimmsten Fall sind alle Daten, die nach der letzten Sicherung geändert wurden, seit der letzten Datensicherung verloren.

Das Medium für die Datensicherung ist ein anderes als das der Originaldaten.

Die Datensicherung wird auf ein externes Medium ausgelagert bzw dupliziert. Das kann eine externe Festplatte, ein NAS oder ein Laufwerk in der Cloud sein.

Worst Case: Wenn das Medium, auf dem sich die Datensicherung befindet, defekt ist, ist die Datensicherung verloren. Eine Datensicherung auf dasselbe Medium zu legen, wie die Originaldaten, ist fahrlässig.

Es gibt mehrere Generationen der Datensicherung.

Die Datensicherung überschreibt nicht die vorhergehende Datensicherung, sondern es sind stets mehrere (mind. eine) Vorversionen verfügbar.

Worst Case: Wenn Daten gelöscht oder verändert werden, enthält die nächste Datensicherung diese Änderung. Oder: Auch eine Datensicherung kann technisch defekt sein, dann ist sie nicht lesbar. Ohne Vorversion gibt es keine Möglichkeit, die ursprünglichen Daten wiederherzustellen.

Das Backup-Medium ist nicht dauerhaft mit dem Rechner verbunden

Das Backupmedium bzw zumindest eine Generation der Backups ist nicht direkt mit dem Rechner verbunden (=angesteckt, verkabelt, online, verbunden etc). Ein Verschlüsselungstrojaner arbeitet sich vom aktuellen Rechner weiter bis zu allen angeschlossenen Laufwerken und Rechnern.

Worst Case: Ein Verschlüsselungstrojaner verschlüsselt nicht nur die aktuellen daten, sondern auch alle erreichbaren Datensicherungen.

Die Datensicherung ist bei Bedarf verschlüsselt und der Zugriff darauf eingeschränkt.

Sensible Daten müssen verschlüsselt werden und der Zugriff darauf muss technisch und organisatorisch eingeschränkt sein. Je nach Daten greifen hier auch Vorschriften der DSGVO.

Worst Case: Die Datensicherung enthält sensible Buchhaltungsdaten, Passwörter, Zugangsdaten oder personenbezogene Daten im Klartext und ist leicht zugänglich. Gerät die Datensicherung in falsche Hände, sind die Daten unmittelbar lesbar und missbräuchlich verwendbar.

Die Datensicherung wird regelmäßig überprüft.

Die Brauchbarkeit der Datensicherung wird regelmäßig getestet, indem eine Wiederherstellung geprobt wird. Zu einer Datensicherung gehört auch ein definierter Prozess zur Wiederherstellung. Das beinhaltet auch die Software zur Wiederherstellung und allfällige Zugangsdaten und Passwörter.

Worst Case: Ein Fehler im Prozess der Datensicherung fällt erst auf, wenn die Datensicherung benötigt wird, aber nicht verfügbar oder nicht brauchbar ist. Oder weil der Prozess zur Wiederherstellung unklar ist.

Es ist klar, wer für die Datensicherung verantwortlich ist.

Für die Datensicherung muss eine verantwortliche Person definiert sein.

Worst Case: Die Fachabteilung verlässt sich auf die IT, die IT weiß nichts von den Daten.

Die Schritte der Datensicherung und der Wiederherstellung sind dokumentiert.

Für die Datensicherung liegt eine schriftliche Prozessbeschreibung vor, diese umfasst auch die Anweisungen zur Wiederherstellung, samt Software, Zugangsdaten und Passwörtern.

Worst Case: Die Datensicherung lässt sich nicht wiederherstellen, weil die Passwörter für den Zugang nicht dokumentiert sind oder die Software zur Wiederherstellung für eine erneute Installation nicht verfügbar ist.

** Ende des Dokuments*