|  |
| --- |
| Thema: Datensicherheit und Datensicherung |
|  |
| 1. Zweck/Geltungsbereich |
| Diese Arbeitsanweisung gibt allgemeine Hinweise für die Datensicherheit und Datensicherung bei Betrieb eines Datenservers.  Datensicherheit:  Grundsätzlich gilt, dass ein professionelles Virenschutzprogramm installiert sein muss, das laufend automatisch aktualisiert wird. Externe Daten von anderen Datenträgern (z.B. USB-Stick, CD, externe Festplatte, etc.) sollten nur nach vorsorglicher Virenprüfung auf den eigenen Server geladen werden.  Für bestimmte Laufwerke oder nur Ordner können unterschiedliche Zugriffrechte freigegeben werden. Damit kann für bestimmte Nutzer (Clients) bzw. Nutzergruppen nur ein Lese- bzw. Schreibzugriff festgelegt werden. Ist der Vollzugriff freigegeben hat der Client das Recht zum Lesen, Verändern (Schreiben) und Löschen von Dateien, womit ggf. das Risiko von unbeabsichtigtem Datenverlust natürlich am größten ist. Üblicherweise dürfen diese Freigaben auf dem Server nur von einem Client mit Administratorenrechten verändert werden.  Datensicherung:  Interne Datensicherung auf Basis des Betriebsystems Windows10. Windows10 erlaubt die Sicherung von Dateiversionen in festgelegtem Zeitabstand. Es werden nur dann Sicherungen erstellt, falls eine neue Version vorliegt. Dabei liegen diese Daten auf dem Server an einem anderen Speicherort (z.B. 2. Festplatte, Festplattenpartition etc.). Alle in dieser Form gespeicherten Dateiversionen können mit einfacher Bedienung sichtbar gemacht werden und stehen für eine ggf. erforderliche Rücksicherung sofort zur Verfügung. Eine Rücksicherung durch eine frühere Version kann z.B. erforderlich sein wenn eine Datei beschädigt wurde, versehentlich Daten gelöscht oder überschrieben wurden oder es zu einer Beschädigung/Sperrung durch Malware (Viren) gekommen sein sollte. Diese Ziele können ebenso durch die Verwendung von Datensicherungsprogrammen und zusätzlichen Festplatten erreicht werden (Backup-Systeme).  Mit Einrichtung einer externen Datensicherung wird das Risiko eines Datenverlustes nach Zerstörung (z.B. Brand) oder Verlust (Diebstahl) des Servers abgesichert. Hierfür muss mit einem Daten­sicherungsanbieter (z.B. Cloud) ein Sicherungsvertrag geschlossen werden. Der Sicherungsanbieter stellt eine dafür geeignete Sicherungssoftware zur Verfügung, welche die Daten über eine Breitbandinternetverbindung auf einen externen Server überträgt. Bei der Installation ist darauf zu achten, dass die Daten nur verschlüsselt übertragen werden. Das Schlüsselkennwort ist 2fach, sicher und für Unbefugte unzugänglich an anderen Orten als dem Serverstandort aufzubewahren. Der Datensicherungsanbieter hat normalerweise keine Möglichkeit ohne das Schlüsselkennwort die verschlüsselten Daten wiederherzustellen. Es empfiehlt sich die Datenrücksicherung testweise einmal auszuprobieren um sich mit dem Programm dafür vertraut zu machen.  Bei Wechsel des Datensicherungsanbieters müssen rechtzeitig vor Ende der Vertragslaufzeit alle möglichen Restoreversionen rückgesichert und an einem anderen Ort archiviert werden, da danach die Daten vom Anbieter gelöscht werden. |
|  |
| 2. Vorgehensweise |
| Einrichtung der internen Datensicherung   * es ist zweckmäßig lediglich eine tägliche Datensicherung einzustellen. Kürzere Sicherungsabstände (z.B. stündlich) würden den erforderlichen Speicherplatz erheblich ansteigen lassen. Sollen Dateiversionen untertäglich gesichert werden kann dies z.B. durch unterschiedliche Dateinamen erreicht werden. * Bei Servern, die im Dauerbetrieb laufen, ist für die Sicherung eine Zeit in der Nacht (z.B. 4:01 Uhr) günstig, weil damit das gesamte Tageswerk des Vortages automatisch gesichert wird und der Server dabei gleichzeitig keine Rechenkapazität für andere Prozesse benötigt. * Die Festplattengröße für die Sicherungskopien ist so groß zu wählen, dass hierfür ein Vielfaches des eigentlichen Datenbestandes zur Verfügung steht. Man bedenke dass der aktuelle Datenbestand rasant anwachsen kann, insb. wenn Fotodokumentationen archiviert werden sollen.   Einrichtung der externen Datensicherung   * Sinngemäß gelten für die externe Datensicherung die selben Einstellungen wie für die interne Datensicherung. * Aus Gründen der Sparsamkeit mit dem gemieteten Speicherplatz gelten für die dauerhafte Archivierung vergangener Zeiträume jedoch stärker ausgedünnte Dateiversionen. So werden i.d.R. aus der laufenden Woche täglich alle 7 Dateiversionen gesichert, im vergangenen Zeitraum von 4 Wochen wöchentlich am Freitag, für 3 Monate rückwirkend monatlich zum 1. des Monats, über 4 Quartale rückwirkend quartalsweise eine Dateiversion zum 1. das Monats, und über 10 Jahre zurück jährlich eine Dateiversion zum 1. das Monats dauerhaft archiviert.   Rücksicherung aus interner Datensicherung   * Im Windows-Explorer die rückzusichernde Datei suchen, rechte Maustaste → Vorgängerversionen wiederherstellen. Es erscheint eine Liste mit Dateiversionen mit verschiedenem Datum und Uhrzeit, gewünschte Datei auswählen. Da die aktuelle Datei mit der Restoredatei überschrieben wird (Speicherung am Originalstandort) ist die aktuelle Version zur Sicherheit vorher auf einen alternativen Pfad umzukopieren, so dass damit vorerst noch die aktuelle Version (verschoben) und die Restoreversion (überschrieben) gleichzeitig auf dem Server vorliegen. Danach kann die Restoreversion auf Funktionsfähigkeit und Informationsgehalt geprüft werden und evtl. mit Daten aus der noch vorhandenen aktuellen Version überarbeitet werden. Erst wenn sicher ist, dass nun mit der bearbeiteten Restoreversion eine verwendbare, reparierte Datei vorliegt, kann die verschobene, defekte, aktuelle Version verworfen werden.   Rücksicherung aus externer Datensicherung   * Prinzipiell gelten hierfür die selben Grundsätze wie für die Rücksicherung aus interner Datensicherung. * Die Rücksicherung erfolgt aber nicht über den Windows-Explorer sondern mit dem Datensicherungsprogramm des Sicherungsanbieters. Hierfür muss dann i.d.R. das Sicherungskennwort eingegeben werden. * Eine komplette Rücksicherung des gesamten Datenbestandes (z.B. bei Wiederaufbau eines zerstörten Servers etc.) kann bei großen Datenmengen u.U. Stunden oder Tage dauern. Ggf. ist es sinnvoll diese Daten vom Sicherungsanbieter auf eine mobile Festplatte kopieren zu lassen und diese anschließend direkt und nicht über die Internetverbindung zu überspielen. |
|  |