Backup: „3-2-1“-Grundsatz

Inhaltsverzeichnis

Versionshistorie

Datum	Bearbeiter	Änderungen
08.04.2020	Markus Freinberger	Dokument erstellen
12.11.2020	Markus Freinberger	Dokument anpassen

Allgemeines

Die „3-2-1“-Regel bezieht sich auf folgende Grundsätze:

- 3 Kopien aller Daten
- Auf 2 verschiedenen Medien(USB-Stick, ext. Festplatte, File-Server/NAS)
- Davon eines außer Haus (zB.: Bankschließfach, bei einem vertrauenswürdigen Feuerwehrmitglied – z.B. Kommandant, im schlimmsten Notfall auf einem externen Cloud-Speicher)

Das wichtigste an einem Backup ist: Ein Backup zu machen!

Wann sollte man ein Backup machen: JETZT!

Im Fall des Falles gilt: Kein Backup, kein Mitleid.

Warum sollte man ein Backup machen?

Die in einer Feuerwehr vorhandenen Daten sind oftmals sehr sensibel (Einsatzdaten, personenbezogene Daten von Mitgliedern, Finanzunterlagen, Schriftverkehre in Dateien und Emails).

Weiters ist ein Verlust (zB. Von Fotos) oft sehr schmerzhaft und vieles unwiederbringlich verloren.

Aufgrund der Tatsache, dass Feuerwehren kritische Infrastruktur darstellen ist ein Backup unabdingbar, zum einen weil es sensible Daten sind (Datenschutz) und zum anderen, weil diese Daten für die tägl. Arbeit der Feuerwehren benötigt und daher geschützt werden müssen (Informationssicherheit/Datensicherheit).

Datenschutz und Datensicherheit sind Teil der digitalen Selbstverteidigung und erhöhen damit die digitale Souveränität der Feuerwehr enorm!

Was kann zum Datenverlust führen?

Es gibt viele Ursachen für Datenverlust. Die häufigsten sind Viren und Computerschädlinge welche Dateien beschädigen, kopieren und an Dritte weiterleiten oder diese Daten oder gar komplette Computersysteme verschlüsseln und damit unzugänglich machen.

Auch Hackerangriffe sind Ursache von Datenverlusten – diese geschehen meist unbemerkt und über lange Zeiträume.

Zwar mit geringer Wahrscheinlichkeit, aber nicht unmöglich sind auch physische Schäden an Computersystemen von Feuerwehren, sei es aufgrund von höherer Gewalt (Wasserschäden, Feuer, Blackout, Überlastungen des Stromnetzes, Blitzschläge,..) oder auch durch z.B. Vandalismus oder Unfälle.

Wir sind doch nur eine kleine Feuerwehr, wer sollte sich für uns interessieren bzw. was ist der Zweck von Hackerangriffen/Virenangriffen?

Hackerangriffe und Viren/Schadsoftware erfolgen gezielt als auch ungezielt. Meist probieren Hacker einfach z.B. bestimmte Ports in einem IP-Adressbereich durch oder finden die Website einer Feuerwehr und testen diese auf Schwachstellen. Durch die so gefundenen Lücken kann der Angreifer dann z.B. Websiten lahmlegen(vergleichsweise harmlos) oder auch auf Serversysteme mit sensiblen Daten (z.B. die Office365-Server von Microsoft) zugreifen.

Die wenigsten Angriffe erfolgen gezielt, meist sind Angriffe auf Feuerwehren oder Vereine „Beifang“ von automatisiert ablaufenden Angriffen auf wahllose Ziele. Gezielte Angriffe sind aber auch bei Feuerwehren nicht auszuschließen und es kann durchaus sein, dass die Feuerwehr von Schaaßklappersdorf gezielt angegriffen wird, sei es aus „Jux und Tollerei“ oder aus anderen Motiven (Bankdaten, Emailadressen, etc..).

Viren bzw. Schadsoftware sind mit einigen Ausnahmen (z.B. Stuxnet, Conficker, etc..) meist ebenfalls nicht auf eine Organisation ausgerichtet sondern soll möglich schnell, möglichst viele Rechner infizieren und je nach Funktion auch Daten abgreifen bzw. selbige Verschlüsseln um Lösegeldforderungen stellen zu können.

Bei dem Angriff eines Verschlüsselungstrojaners oder eines Schädlings der Festplatten formatiert ist ein Backup ein notwendiger Sicherheitsanker. So können (wenn auch die Systeme neu aufgesetzt und konfiguriert werden müssen) zumindest die Daten wiederhergestellt werden.

Wie sollte ein Backup erfolgen?

Das Sichern der Daten sollte in einem offenen und dokumentierten Format erfolgen(z.B. als sog. „Tar-Ball“ oder als zip-Datei) bzw. sollten die Daten auch einfach 1:1 auf ein Sicherungsmedium kopiert werden - am besten auf verschlüsselten Datenträgern, so kann bei einem Diebstahl von Festplatten bzw. der Sicherungsmedien nicht auf die Daten zugegriffen werden.

Von Backup-Software die die Daten in irgendwelchen Container-Formaten oder eigenen Dateiformaten ablegt ist abzuraten, denn wenn man die Software nicht mehr hat oder eine neue Version das alte Format von 2019 nicht mehr unterstützt kommt man nicht mehr an die gesicherten Daten!

Was sollte gesichert werden?

Kurz: Alles was für die Feuerwehr von Relevanz ist.

Das sind im groben:

- Emails (viele Emailprogramme wie Thunderbird, Evolution oder Outlook bieten den Export von Postfächern oder zumindest ein simples kopieren selbiger an)
- Feuerwehr-interne Dokumente (Übungspläne, Schlüssellisten, etc..)
- EDV-Dokumente (Dokumentationen von Systemen, Anleitungen, Lizenz-Listen, etc..)
- Datenbanken sofern vorhanden (z.B. die Datenbank der Website oder Passwortdatenbanken,etc..)
- Schriftverkehr und Dokumente(z.B. Behördenkorrespondenz, Schriftverkehr mit AFK/BFK/LFK)
- Finanzdaten (Rechnungen, Kostenersätze, etc..)
- Fotos von Einsätzen, Veranstaltungen,etc..

In welchen Zeitabständen sollte gesichert werden?

Hier gibt es keine genaue Regel, da sich manches nicht so oft ändert (z.B. Passwortdatenbanken) wie anderes (z.B. Emailpostfächer).

Grundsätzlich muss hier jede Feuerwehr selbst entscheiden wie oft gesichert werden soll.

Es empfiehlt sich aber zumindest wöchentlich zu sichern, so ist im Fall des Falles „nur“ eine Woche verloren. Die Sicherung auf einen externen Datenträger der außer Haus gelagert wird, erfolgt einmal im Monat.

Das Backup im Detail

Die Daten der FF Musterhausen liegen auf einer eigenen internen Festplatte am Büro-PC im Gerätehaus. Diese Daten werden einmal pro Woche auf eine externe Festplatte kopiert, diese Festplatte liegt in einem versperrbaren Kasten im versperrbaren Büro im Gerätehaus.

Einmal im Monat werden die Daten auf eine zweite externe Festplatte kopiert, welche danach wieder beim Feuerwehrkommandanten gelagert wird.

Erklärung:

Die **3** Kopien der Daten befinden sich:

- Auf dem PC im Büro
- Auf der externen Platte im Büro
- Auf der externen Platte beim Feuerwehrkommandanten zuhause

Die **2** unterschiedlichen Medien sind:

- die beiden ext. Festplatten

Dadurch ist eine Kopie zwar im Falle eines Datenverlustes auf dem PC verloren, die Daten auf den ext. Festplatten stehen aber zur Verfügung.

Die ext. Festplatte die im Haus des Feuerwehrkommandaten gelagert wird steht für den **1er** in der „3-2-1“-Regel.

Da diese Festplatte nicht am selben Ort wie der PC und die erste Sicherung liegt, kann auch auf eine Sicherheitskopie der Daten zugegriffen werden wenn beide anderen Kopien nicht mehr vorhanden sind.

Wichtig ist auch regelmäßig zu testen ob sich die Daten wiederherstellen lassen bzw. auch öffnen lassen und nicht beschädigt sind. Denn das Beste Backup nutzt nichts, wenn die Sicherung kaputt ist!

Empfohlene Infrastruktur

Grundsätzlich empfiehlt es sich die Daten möglichst nicht aus der Hand zu geben, daher werden in diesem Dokument Clouddienste der diversen Einschlägigen Anbieter (OneDrive, Amazon, Dropbox, etc..) ausdrücklich nicht empfohlen – und sofern diese genutzt werden, so sollten diese Daten immer verschlüsselt (mind. als zip-Datei mit einem Passwort oder noch besser in verschlüsselten Containern mit VeraCrypt) in Clouddienste hochgeladen werden (JA – auch in OneDrive vom LFV).

Für die einfachste Umsetzung eines robusten Backups genügen zwei externe Festplatten mit ausreichender Kapazität sowie ein geeigneter Ort (versperrbarer Schrank, Tresor, externer Lagerort).

Steht ein fachkundiger EDV-Sachbearbeiter zur Verfügung wäre ein zentrales NAS (=Network Attached Storage) eine Möglichkeit die Daten dort als 2. Kopie abzulegen und automatisiert (z.B. beim Runterfahren des PCs) auf dieses NAS zu speichern.

Hierfür empfiehlt sich die freie, offene NAS-Software „FreeNAS“ die mit der Cloud-Software „Nextcloud“ erweitert wird. Damit kann ein interner Datenserver eingerichtet werden, der sich einfach und sehr gut administrieren lässt und bei Bedarf über die Erweiterung „Nextcloud“ Daten fein granuliert extern verfügbar machen kann.

Alternativ bietet sich hier auch ein gehärteter Debian oder Ubuntu-Server an auf dem entsprechende Netzwerk-Freigaben eingerichtet werden.

Wichtig bei der Variante mit NAS ist: auch diese Geräte gehören regelmäßig gewartet und aktualisiert!

Grundsätzlich gilt jedoch das KISS-Prinzip! Man muss die Dinge nicht komplizierter machen als sie sind.

Empfohlene Programme

Bei der Backupsoftware sind grundsätzlich ebenso freie und offene Programme zu bevorzugen, da dadurch sichergestellt ist, dass nachvollzogen werden kann was das Programm macht und man sich an gängige Standards hält.

Für Windows-Rechner:

- Personal Backup (sichert die Daten als 1:1 Kopien oder als komprimierte zip-Dateien, nicht frei und offen, aber kostenlos, windows-only)
- Robocopy (kostenloses Kommandozeilen-Programm von Microsoft, unfrei, windows-only)
- 7zip (freie, offene Archiv-Software, für Windows und Linux)
- Veracrypt (freie, offene Software für Festplattenverschlüsselung bzw. zum erstellen verschlüsselter Container, Linux und Windows)

Für Linux-Rechner:

- rsync (freies, offenes Kommandozeilen-Programm, kostenlos, für Windows, Mac und Linux)
- tar (freies, offenes Kommandozeilen-Programm, kostenlos, Linux/UNIX only); Beispiel für eine Tar-Sicherung einer Nextcloud
- p7zip (Portierung für Linux von 7zip, frei und opensource, Linux)
- Veracrypt (freie, offene Software für Festplattenverschlüsselung bzw. zum erstellen verschlüsselter Container, Linux und Windows)

Literaturverzeichnis / Nützliche Links

[1] https://www.heise.de/select/ct/2018/20/1537842151930716, abgerufen am 30.11.2020

[2] https://blog.jakobs.systems/blog/nextcloud-datensicherung-mit-tar/, abgerufen am 30.11.2020

[3] https://www.kuketz-blog.de/slugmap/#Backup, abgerufen am 30.11.2020

KONTAKT
Freiwillige Feuerwehr Texing
Altendorf 32
A-3242 Texingtal

Email: n12114@feuerwehr.gv.at
Web: https://www.feuerwehr-texing.at