



Backup statt Lösegeld

Daten Trojaner-sicher speichern

Wohin am besten sichern Seite 102
Backup mit Duplicati Seite 108
Backup-FAQ Seite 114

Klar kann man es mit „Daumen drücken“ probieren, aber der einzig wirklich zuverlässige und zugleich praktikable Schutz vor den derzeit kursierenden Erpressungstrojanern ist ein Backup. Das klingt schwieriger, als es ist – mit wenigen Mausklicks sind Ihre Daten in Zukunft Trojaner-sicher.

Von Gerald Himmelein, Lutz Labs und Axel Vahldiek

Die Gefahr, als Otto Normalbürger Opfer einer Erpressung zu werden, ist heutzutage so groß wie noch nie: Kriminelle verbreiten seit einiger Zeit immer wieder neue Trojaner, die die persönlichen Daten auf PCs so verschlüsseln, dass damit niemand mehr etwas anfangen kann. Erst nach Zahlung eines Lösegelds rücken die Kriminellen den Schlüssel heraus, mit dem die Daten wieder lesbar werden – meistens jedenfalls. Denn um die Zahlungsmoral der Opfer hochzuhalten, ist es zwar durchaus im Interesse der Verbrecher, dass das Entschlüsseln zuverlässig klappt, doch mitunter stecken Bugs in der Entschlüsselungssoftware oder der Schlüssel kommt beim Opfer gar nicht erst an. Und dann sind die Daten unrettbar verloren.

Schützen kann man sich vor den Erpressern auf unterschiedlich wirksamen Wegen. In großen Unternehmen setzen Admins gern Positivlisten ein: Ein Programm auf dem Rechner eines Mitarbeiters läuft nur dann, wenn das von den Admins ausdrücklich erlaubt wurde.

Für kleinere Firmen und erst recht für Privatanwender, die immer wieder andere Anwendungen einsetzen wollen, ist die aufwendige Pflege so einer Liste inklusive der dazugehörigen Zertifikate und Prüfsummen aber kaum praktikabel. Der Plan B besteht hier üblicherweise im Verstopfen der Schlupflöcher, durch die die Trojaner eindringen könnten. Reichlich Tipps dazu standen gerade erst in [1], doch wie wir schon dort schrieben: „Die drei wichtigsten Tipps zum Schutz vor Erpressungs-

trojanern lauten: Backups, Backups, Backups“.

Dazu hatten wir seinerzeit auch ein paar Tipps gegeben, doch zahlreiche Leser haben sich in Rückmeldungen eine ausführlichere Behandlung des Themas gewünscht. Et voilà: Hier ist sie. Dieser Artikel stellt Speicherziele fürs Backup vor, die sicher vor Erpressungstrojanern sind. Und ab Seite 108 zeigen wir am Beispiel des Backup-Programms Duplicati, wie Sie ganz einfach und mit wenigen Mausklicks einen Backup-Job konfigurieren, um den Sie sich nach der Einrichtung kaum noch kümmern müssen. Weitere Fragen zum Thema Backup beantworten wir in einer FAQ ab Seite 114.

Backup-Ziele

Um vor dem direkten Zugriff eines Verschlüsselungstrojaners sicher zu sein, müssen Backups auf einem Medium landen, auf das der aktuelle Benutzer keinen direkten Zugriff hat. Das klingt zunächst nach einer unmöglichen Voraussetzung: Irgendwie muss das Backup-Programm ja Verbindung nach draußen aufnehmen.

Die einfachste, wenn auch vielleicht die unkomfortableste Möglichkeit ist eine externe Festplatte: Einfach anstecken und Backup starten. Während es läuft, schließt man Browser und Mailprogramm besser, denn diese Programme sind die häufigsten Einfallswegen für Erpressungstrojaner. Wenn das Backup beendet ist, kommt die Platte wieder an einen Ort, der idealerweise möglichst weit vom eigenen PC entfernt ist – so sind die Daten auch im Falle

eines Einbruchs oder Feuers noch sicher. Ist der Rechner bereits infiziert, könnte der Erpressungstrojaner allerdings während des Backups zuschlagen und sämtliche Sicherungen verschlüsseln.

Des Weiteren eignen sich als Ziel für das Backup alle per Netz erreichbaren Medien, die für das Beschreiben die Angabe von Benutzernamen und Passwort verlangen. Wer seine Dateien gerne im eigenen Heimnetz behalten möchte, kann dafür ein NAS nutzen, selbst mit der Fritzbox als Ziel klappt es.

Auch FTP-Zugänge des eigenen Webhosting-Angebots oder andere Cloud-Dienste bieten sich an. Im Idealfall nutzt man nicht nur eines dieser Ziele, sondern mehrere – wie Sie die einzelnen Backup-Ziele einrichten und möglichst komfortabel nutzen, erläutern wir im Folgenden.

Ach, und ein weiteres Locky-sicheres Ziel wollen wir nicht unterschlagen, auch wenn es in den letzten Jahren immer mehr an Bedeutung verloren hat: Man kann seine Daten auch auf CD-ROM, DVD oder Blu-ray brennen. Wenn sie einmal dort gespeichert sind, kann sie niemand mehr verändern. Irgendwo findet sich bestimmt noch die Spindel mit den Rohlingen ...







Einfach mal machen

Man kann sich viele Stunden mit der optimalen Strategie für ein Backup beschäftigen. Am besten aber greifen Sie **jetzt** zu einer externen Festplatte oder suchen den Stapel mit den Rohlingen. Dann sichern Sie einfach mit dem Windows-Explorer den Ordner „Eigene Dateien“. Damit haben Sie vielleicht nicht alle Dateien erwischt, aber wahrscheinlich die wichtigsten – und jedes Backup ist besser als gar kein Backup.

Nachdem das erledigt ist, gehts zu den Feinheiten: Wie Sie das Backup mit den wichtigen Daten möglichst komfortabel vor Locky & Konsorten verstecken.

Externe Festplatten

Festplatte einstecken, Backup starten und danach wieder abziehen – das ist zwar einfach, aber unkomfortabel. Zwei pragmatische Tipps dazu: In beiden Fällen gehen wir davon aus, dass sich das Backup-Programm wie das im nächsten Artikel vorgestellte Duplicati per Skript starten lässt oder eine Option enthält, vor und nach dem Backup-Job ein Skript zu starten. Die

Trojaner-sichere Backup-Ziele						
Medium	USB-Festplatte	NAS	USB-Platte am Router	Dropbox & Co.	Webspace	DVD
						
automatisierbar	–	✓	✓	–	✓	–
Geschwindigkeit abhängig von	USB-Komponenten	Netzwerk/Gerät	Router	Internet-Anschluss	Internet-Anschluss	Brenngeschwindigkeit
Backup automatisch an anderem Ort	–	–	–	✓	✓	–
Backup während der Sicherung geschützt	–	✓	✓	✓	✓	✓
Bemerkungen	sicherer und automatisierbar mit Schalter	optimale Lösung für das Heimnetz	meistens recht langsam	nur ohne Client einsetzbar, geringe Kapazität	hohe Kapazitäten teuer	Kapazität einzelner Medien begrenzt
✓ vorhanden – nicht vorhanden						

Backup-Platte kann dabei eingesteckt bleiben.

Für den ersten Tipp brauchen Sie keine zusätzliche Hardware: Die Festplatten – ob nun per USB verbunden oder intern am SATA-Port angeschlossen – bleiben verbunden, werden aber über die Datenträgerverwaltung von Windows offline geschaltet und sind damit nicht mehr erreichbar. Dazu reichen die folgenden Diskpart-Befehle aus:

```
select disk <Nummer>
offline disk
```

Vor dem Backup muss die Platte online geschaltet werden:

```
select disk <Nummer>
online disk
```

Diese Befehle schreibt man in zwei Textdateien, etwa mit den Namen disk-on.txt und disk-off.txt und übergibt sie dem Windows-Tool Diskpart in einer mit Administratorrechten laufenden Kommandozeile:

```
diskpart /r disk-on.txt
```

Die Nummer des Laufwerks müssen Sie einmalig über die Datenträgerverwaltung auslesen. Achtung: Wenn Sie zusätzliche Festplatten in den PC einbauen oder ein USB-Stick am PC steckt, kann sich die Nummer der Backup-Festplatte ändern. Dann versucht das Skript eventuell, das falsche Laufwerk zu aktivieren.

Ein Trojaner könnte allerdings schauen, ob sich offline geschaltete Festplatten im System befinden und diese auf dem beschriebenen Weg reaktivieren – vielleicht lesen die Kriminellen ja auch c't.

Tipp Nummer zwei ist das Abschalten der Versorgungsspannung. Wenn Sie so-

wieso den Kauf eines externen Backup-Laufwerks planen, achten Sie darauf, ein Modell mit einem Netzschalter zu erwischen. So brauchen Sie lediglich den Schalter umzulegen, um dem Trojaner den Weg zu den Dateien zu versperren.

Die meisten USB-Platten im 2,5-Zoll-Format haben zwar keinen Schalter, aber auch diese lassen sich abschalten. Passende USB-Schalter hat etwa das deutsche Unternehmen Cleware unter dem Namen USB Connect im Programm.

Diese Schalter gibt es in verschiedenen Versionen, per USB steuerbar und mit und ohne Taster. Unser 65 Euro teures Testmuster lässt sich auf beide Arten schalten. Der Hersteller stellt Software zur Steuerung zur Verfügung, darunter auch APIs zum Einbinden in eigene Programme. Mit einem einfachen Kommandozeilen-Utility lassen sich die externen Laufwerke über Batch-Dateien ein- und ausschalten. Hat man mehrere USB-Schalter im Einsatz, lassen sich diese über die auf der Unterseite der Schalter aufgedruckte Seriennummer ansprechen.

Cleware liefert zu den Schaltern USB-Kabel mit jeweils einem Typ-A-Stecker am Ende mit – das ist eigentlich nicht USB-konform, aber egal: Auch das Ausschalten eines USB-Gerätes über einen Schalter außerhalb des PCs ist offiziell nicht gestattet. Eine externe Festplatte aus unserem Testfundus kam mit der verlängerten Zuleitung auch nicht klar: Das Seagate Plus Portable Drive schaltete sich zwar ein, im Windows-Explorer aber tauchte das Laufwerk immer nur für wenige Sekunden auf, bevor es sich wieder abmeldete. Mit anderen Festplatten, externen SSDs sowie diversen USB-Sticks trat dieses Problem nicht auf. Das Abschalten des Laufwerks

über den Schalter funktionierte im Test auch bei einer Festplatte mit eigener Stromversorgung – das muss aber nicht für alle Modelle dieser Art gelten.

In einem Skript lässt sich das externe Laufwerk über

```
USBSwitchCMD <Nummer des Schalters> 0|1
```

steuern. Die Nummer des Schalters benötigt man nur, wenn mehrere USB-Schalter am PC angeschlossen sind, der Parameter 0 kappt die Verbindung, 1 schließt sie wieder.

Auch beim USB-Schalter könnte ein Trojaner-Entwickler auf den Gedanken kommen, nach dem Vorhandensein einer solchen Software zu forschen und anschließend in Batch-Dateien nach dem passenden Befehl zum Freischalten suchen – aber das ist derzeit wohl noch als hypothetisch einzustufen. Die beiden Methoden lassen sich auch kombinieren: Erst offline schalten, dann abschalten. Windows merkt sich, dass ein Laufwerk offline ist; auch nach dem Wiedereinschalten der Stromversorgung muss man das Laufwerk also erst online schalten, um darauf zugreifen zu können.

Im Extremfall kann es passieren, dass Locky zuschlägt, während gerade ein Backup läuft; der Trojaner also diesen Moment abwartet und dann alle Backups löscht. Daher kann es nicht schaden, die Daten nicht nur auf einer Festplatte zu sichern, sondern auf zwei Laufwerken im Wechsel. So sind die Daten nicht nur für den eben genannten Fall sicher; auch ein Laufwerksausfall verliert den Schrecken.

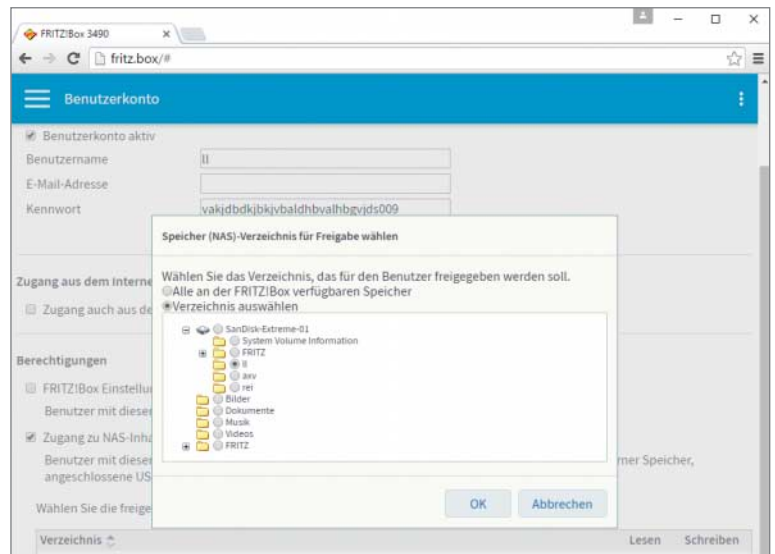
Festplatte an der Fritzbox

Ohne An- und Abstöpseln oder Skripte zum Ein- und Ausschalten der Sicherungs-

laufwerke kommt man aus, wenn das Backup-Ziel für das Beschreiben die Angabe von Benutzername und Passwort fordert. Hierfür gibt es verschiedene Möglichkeiten, etwa kennwortgeschützte FTP-Zugänge oder Freigaben mit eigenen Benutzernamen und Passwort. Einige Router bieten die Möglichkeit, solche Zugänge für eine am USB-Port hängende Festplatte einzurichten. Viele Nutzer haben einen solchen Router bereits im Haus, nämlich eine der in Deutschland recht beliebten Fritzboxen.

Diese hat einen USB-Anschluss, an dem sich eine Festplatte oder ein USB-Stick anschließen lässt. Diese Laufwerke lassen sich auch per FTP befüllen, die Zugänge dafür richtet man über die Fritzbox-Oberfläche ein. Das funktioniert, ist aber recht langsam: Bei einer Fritzbox 7390 mit USB-2.0-Schnittstelle konnten wir per LAN gerade einmal 5 MByte/s auf einen schnellen USB-Stick übertragen, bei einer Fritzbox 3490 mit USB 3.0 waren es immerhin 11 MByte/s. Einfache NAS sind weit schneller, 60 MByte/s und mehr haben wir bei einigen Geräten schon gemessen. Doch ein langsames Backup ist allemal besser als gar kein Backup.

Vor dem Einrichten der Benutzer auf der Fritzbox empfiehlt es sich, das USB-Laufwerk einmal an einen Windows-PC anzuschließen und dort Verzeichnisse für



Über die Web-Oberfläche legt man für jeden Nutzer der Fritzbox ein eigenes Backup-Verzeichnis an.

die einzelnen Nutzer zu erstellen, denn das klappt über die Fritzbox-Oberfläche nicht. Die Benutzer selbst richtet man bei der Fritzbox über das Systemmenü ein; jeder Nutzer erhält nur Zugriff auf sein Benutzerverzeichnis.

Bei der Fritzbox ist jedoch Vorsicht geboten: Mit den FTP-Zugangsdaten kann man auch auf die SMB-Freigabe der Fritzbox (standardmäßig als \\fritz.box eingerichtet) zugreifen. Windows speichert die

Anmeldedaten auf Wunsch – einige Erpressungstrojaner suchen im lokalen Netz nach beschreibbaren Freigaben und verschlüsseln auch die dort liegenden Dateien. Wer den Zugriff auf die Fritzbox-Freigabe benötigt, sollte daher besser einen weiteren Benutzer in der Fritzbox anlegen, der lediglich Leserechte darauf hat.

Falls Ihnen übrigens das Design der Fritzbox-Oberfläche im Bild oben unbekannt vorkommt, sollten Sie mal ein Sys-

Anzeige

tem-Update anstoßen. Für viele Modelle ist bereits die Version 6.51 verfügbar.

Sicher im NAS

Bei großen Datenmengen ist die Fritzbox schnell überfordert, und eigentlich eignen sich für diese Aufgabe spezielle Geräte so wieso viel besser. Ein NAS, also eine ins Heimnetz eingehängte Box mit einer oder mehreren Festplatten und einem speziell auf die Speicherung von Dateien optimierten Betriebssystem, stellt jedem Backupwilligen Mitglied des Haushalts ein eigenes, kennwortgeschütztes Verzeichnis bereit, das nur diesem einen Benutzer beziehungsweise Rechner zugänglich ist. Sind an einem PC regelmäßig mehrere Nutzer angemeldet, sollten diese eigene Sicherungsverzeichnisse erhalten.

Im nächsten Schritt wird das Backup-Programm angehalten, seine Sicherungen in das Verzeichnis auf dem NAS zu schreiben. Die Zugangsdaten erhält dabei ausschließlich das Backup-Programm; der Benutzer des Rechners hat hingegen keinen direkten Zugriff auf die Daten.

Die folgenden Schritte spielen das Szenario am Beispiel des Mini-NAS WD My Cloud durch. NAS-Modelle von Synology & Co. lassen sich ähnlich konfigurieren. Erster Schritt sollte eine Aktualisierung der Firmware sein.

Jetzt wird in den Einstellungen deaktiviert, was das NAS von außen angreifbar machen könnte, also vor allem der Remote-Zugriff. Deaktivieren Sie alle Dienste, die Sie nicht benötigen, etwa Time-Machine-Backups oder den DLNA-Server. Jetzt aktivieren Sie unter „Netzwerk/Netzwerkdienste“ den FTP-Zugriff.

Weiter gehts unter „Benutzer“: Hier richten Sie so viele Benutzer ein, wie Rechner zu sichern sind. Geben Sie den Benutzern sprechende Vornamen, etwa „HaenselPC“ oder „GretelBook“, und sichern Sie die Zugänge mit einem Passwort. Nun geht es an die Freigaben. Hier löschen Sie alle vorkonfigurierten Freigaben bis auf Public. Legen Sie neue Freigaben an, bei denen Sie sich an den Benutzernamen orientieren, etwa „bkhaenselpc“.

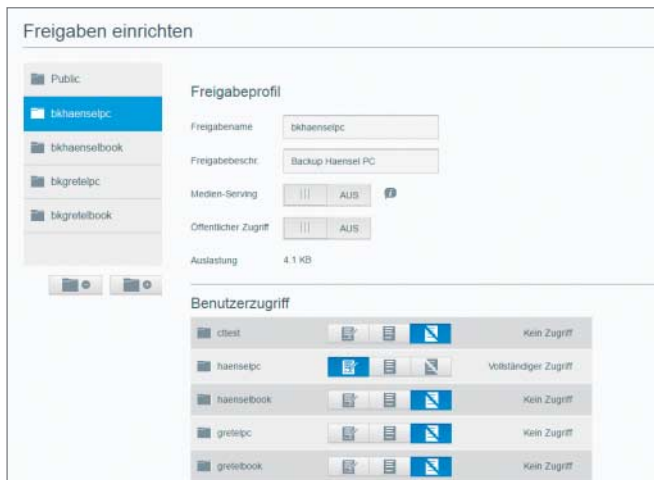
Konfigurieren Sie für jede Freigabe den Benutzerzugriff. Dazu klicken Sie in der Liste links auf den Namen der Freigabe, schalten unter „Freigabeprofil“ den „Öffentlicher Zugriff“ aus und klicken dann die Einträge unter der Überschrift so zurecht, dass nur der richtige Benutzer darauf lesen und schreiben darf.

Der Vollständigkeit halber sei daran erinnert, dass Sie die Benutzernamen, Kennwörter und Freigabenamen an einer sicheren Stelle dokumentieren müssen – etwa in einem Passwort-Manager oder auf einem garantiert trojanersicheren Blatt Papier. Am besten tun Sie beides.

Backup in die Cloud

Ein Trojaner-sicheres Backup lässt sich auch in der Cloud ablegen. Sogar Dropbox & Co. eignen sich – mit etwas Vorsicht: Am besten nutzt man dazu die Web-Oberfläche der Dienste und schiebt die Dateien per Drag & Drop in die Cloud. Denn wenn man den zugehörigen Client installiert und der Trojaner auf der eigenen Festplatte zuschlägt, würde der Dienst die nun unzugänglichen Dateien in die Cloud synchronisieren. Zwar versprechen die An-

Um das NAS WD My Cloud als Locky-sicheren Backup-Server zweckzuentfremden, legt man für jeden zu sichernden Rechner einen eigenen Benutzer mit Kennwort an, der allein auf die für ihn vorgesehene Freigabe zugreifen darf.



Jede Freigabe wird einem und nur einem Benutzer zugeordnet. In die anderen Freigaben darf nicht einmal der Administrator hineingucken.

bieter Backups der Daten von mindestens 30 Tagen, doch darauf verlassen sollte man sich nicht.

Für größere Backups sind diese Dienste aber schon aufgrund ihrer Größenbeschränkung auf wenige GByte unbrauchbar. Andere Cloud-Ziele sind allerdings meistens nicht kostenlos zu haben. Wer schon eine eigene Homepage im Netz betreibt, braucht keinen Cloud-Speicher: In den meisten Webspace-Angeboten und erst recht bei eigenen Webservern sind diverse GByte Speicherplatz dabei, die per FTP – oder besser noch per Secure FTP – befüllt werden können. Die Verzeichnisse sollten jedoch nicht öffentlich zugänglich sein, deshalb sichert man sie über eine .htaccess-Datei gegen unerwünschte Zugriffe aus dem Netz ab.

Weiter gibt es eine Reihe reiner Onlinespeicher-Angebote – die meisten aber sind nicht per FTP erreichbar. Eine Ausnahme ist das HiDrive von Strato; das kleinste Paket mit 20 GByte Speicherplatz für monatlich weniger als einen Euro reicht für viele Fälle schon aus. Ärgerlich nur, dass Strato für den FTP-Zugang einen Aufschlag von 5 Euro pro Monat verlangt.

FTP ist jedoch nicht der einzige Weg, seine Daten in der Cloud zu sichern. Einige Onlinespeicher-Angebote lassen sich per WebDav befüllen, andere per rsync, sogar das Profispeicher-Angebot Amazon S3 ist eine Alternative. Wichtig ist nur, dass das verwendete Backup-Programm diese Standards direkt unterstützt. Nur so kommt man ohne zusätzlichen Client aus, der eventuell doch wieder eine Sicherheitslücke in das Konzept reisst. Wer etwa regelmäßig Betriebssystem-Images si-

chern möchte, sollte sich mit einer FTP-Alternative wie rsync beschäftigen, die nur die Veränderungen einer Datei überträgt – das steinalte FTP hingegen würde die mehrere GByte große Image-Datei einfach komplett neu sichern.

Beim Backup in die Cloud sollte man jedoch auf jeden Fall seine Daten verschlüsseln, denn niemand kann garantieren, dass sich nicht doch einmal ein neugieriger Admin darüber her macht. Das erledigen Backup-Programme wie das im folgenden Artikel vorgestellte Duplicati automatisch. Ansonsten gelten die gleichen Vorsichtsmaßnahmen wie im lokalen Netz: Der FTP-Zugang darf nur für das Backup genutzt werden und ein Abgleich über einen separaten Windows-Client ist tabu.

Und nun automatisch

Eine ganze Reihe von Locky-sicheren Zielen für die wichtigsten Arbeitsdateien, die Urlaubserinnerungen und die Steuererklärung haben wir Ihnen in diesem Artikel vorgestellt. Im folgenden Artikel möchten wir Ihnen nun die Einrichtung von Duplicati näher bringen. Dieses Backup-Programm ist kostenlos, und nach der recht einfachen Einrichtung brauchen Sie sich kaum noch um das Sichern der Daten zu kümmern. Und wenn dann doch mal ein Trojaner zuschlägt: Keine Panik, es gibt ein Backup – Lösegeld müssen Sie nicht zahlen.

(ll@ct.de) **ct**

Literatur

- [1] Ronald Eikenberg, Erpresser-Schutz, Windows und Daten gegen Erpressungs-Trojaner wappnen, c't 7/16, S. 78

Anzeige