Langmeier Backup

Best Practices zum Schutz vor Ransomware

Ransomware: Gefahrenlage

Ransomware ist immer noch die größte Bedrohung im Netz. Cybererpresser verschlüsseln dabei alle Daten und Dokumente. Sie bieten dann vermeintliche Entschlüsselung nach Lösegeldzahlung an – oftmals jedoch nur gefaked. Daher sollte man solche Lösegeldforderungen auch nicht zahlen!

Das Vorgehen von Ransomware ist meistens wie folgt: Erst werden die lokalen Laufwerke durchsucht und alle Dokumente verschlüsselt, dann angeschlossene Laufwerke wie USB-Sticks und schließlich sogar alle erreichbaren Netzwerkfreigaben. Hierbei werden dann gegebenenfalls auch Backups verschlüsselt. Ein Desaster, da so keine einfache Rücksicherung möglich ist.

Ransomware: Ansatzpunkte zur Abwehr

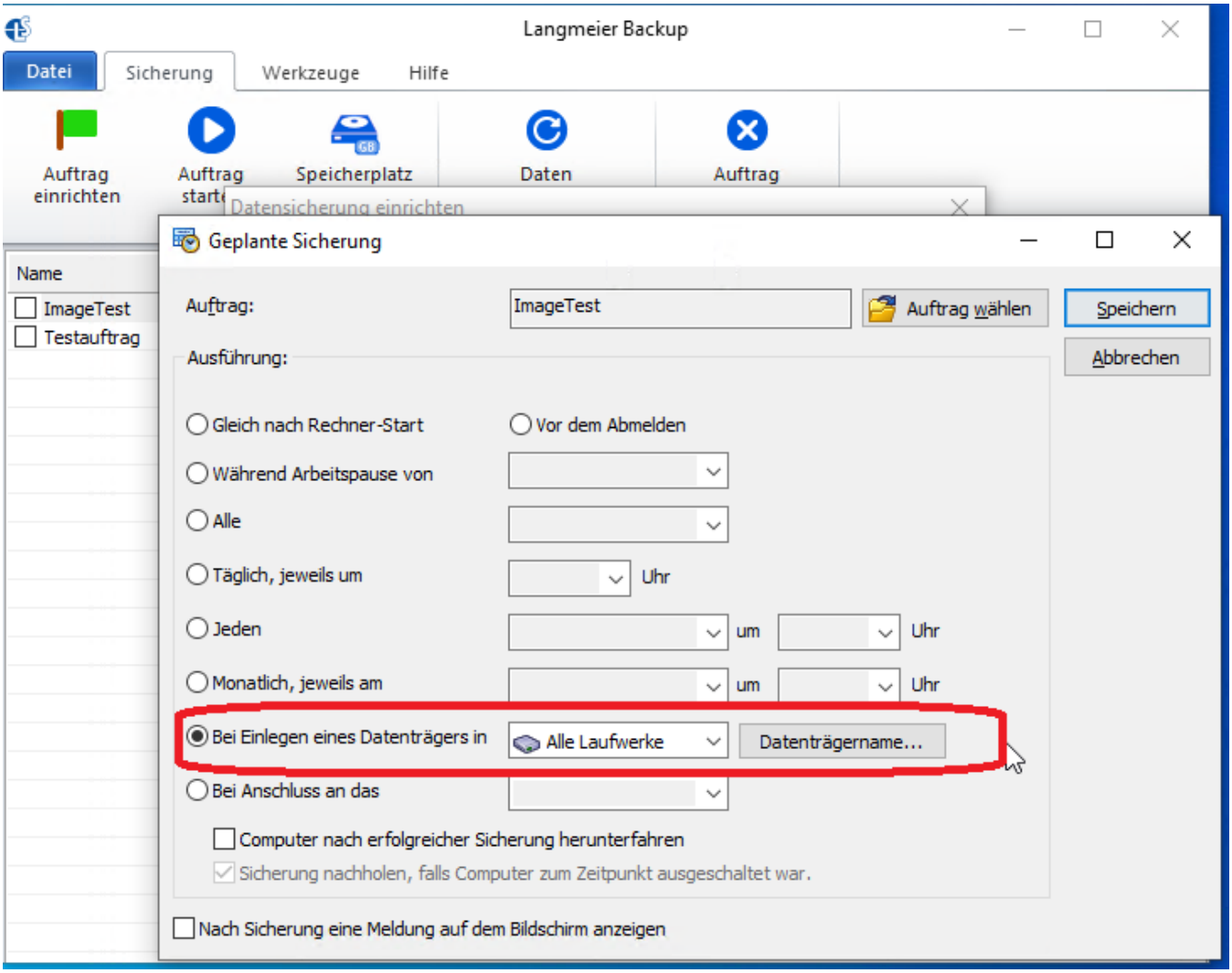
Um Ransomware abzuwehren, muss man ein Sicherheitskonzept umsetzen. Es umfasst einen aktuellen Virenschutz, Schulung der Mitarbeiter und schließlich ein aktuelles Backup, regelmäßig ausgeführt und vor Zugriffen der Ransomware geschützt.

Man sollte die Backups vor dem Ransomware-Zugriff schützen. Dabei gibt es nur wenige Möglichkeiten: Zum einen kann man das Backup-Medium (etwa USB-Stick) nur für das Backup selber angesteckt lassen, also physikalische Trennung. Zum anderen hilft die Einrichtung eines Backup-Administrator-Kontos, das als einziges Zugriffsrechte auf die Backups hat.

Ransomware: Backups schützen in der Praxis

Langmeier Backup Essentials ist für die vereinfachte Bedienung stark abgespeckt im Funktionsumfang. Daher bietet sich hier an, die physikalische Trennung durch den Nutzer zu verfolgen. Das heißt, das Backup-Medium (etwa USB-Stick) nur für das Backup selber angesteckt zu lassen.

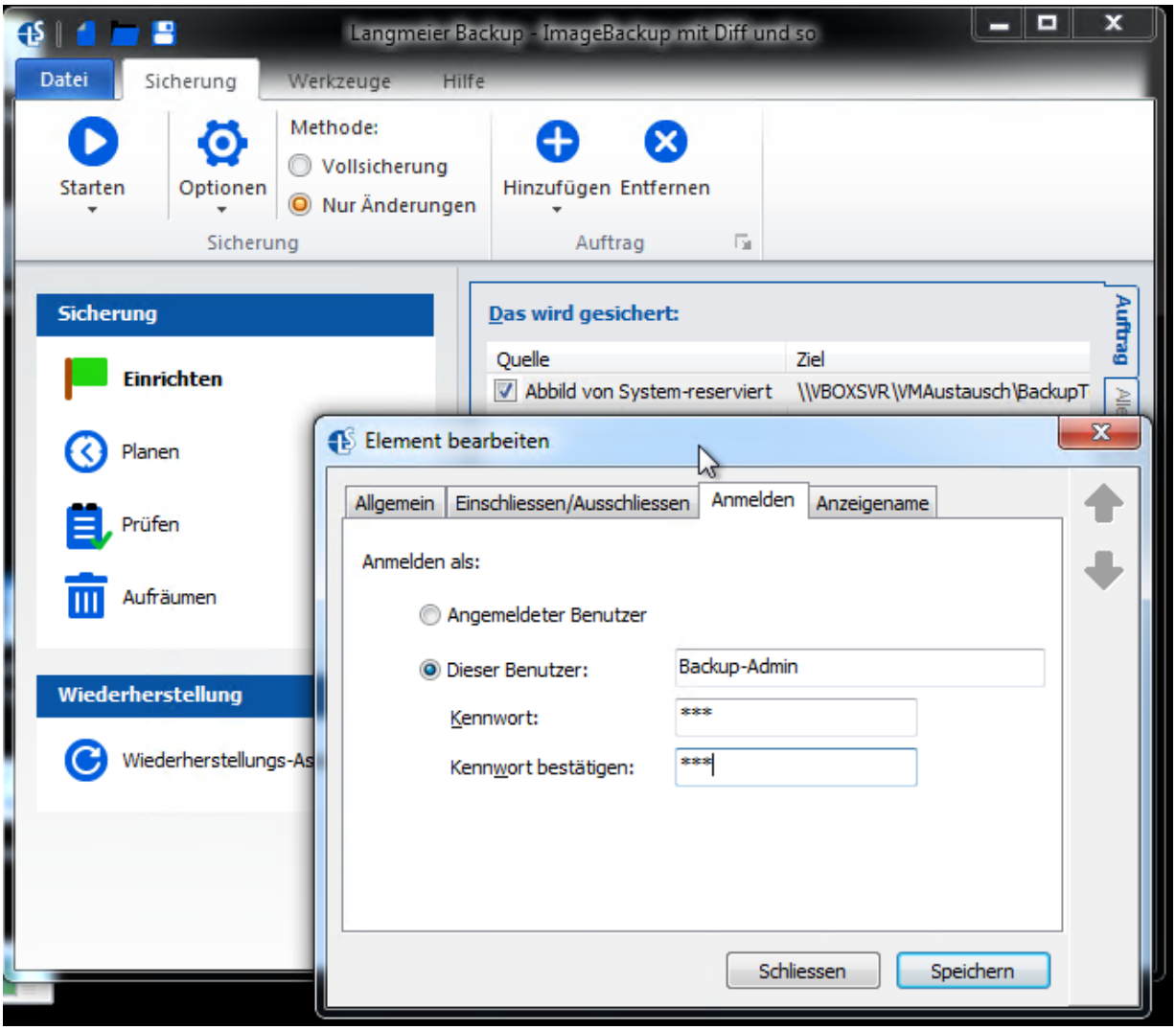
Der Backup-Job wird via Zeitplan so eingerichtet, dass beim Anstecken des Laufwerks das Backup gestartet wird. Nach dem Backup (beispielsweise am folgenden Morgen) zieht der Nutzer das USB-Laufwerk ab. Seit Windows 10 Build 1903 ist die Voreinstellung in Windows so, dass durch das direkte Abziehen ohne vorheriges Auswerfen im Betriebssystem kein Datenverlust droht.



Ab Langmeier Backup Business stehen fortgeschrittene Funktionen wie das Arbeiten als Dienst mit bestimmtem Benutzer-Zugang oder die gezielte Anmeldung in einem Backup-Auftrag als bestimmter Nutzer bereit.

Hier empfiehlt sich als optimierte Lösung, einen Backup-Administrator als Zugang einzurichten. Auf dem NAS hat dieser Benutzer Zugriffsrechte Schreibend auf das freigegebene Backup-Verzeichnis; auf dem lokalen Rechner Admin-Rechte. Da Ransomware im Benutzerkontext läuft, kann sie Backups so nicht erreichen und verschlüsseln.

So lässt sich die Anmeldung im Backup-Auftrag nutzen:



Weitere Informationen zu Langmeier Backup finden Sie unter:
https://www.jakobsoftware.de/langmeier

Stand: 08/2020