

# Simple Ransom Safe Backup Tool

V01.00 - 15.12.2025

## Inhalt

- Aufgabe ..... 2
  - Was ist eine Ransomware-Attacke? ..... 2
  - Wie schützt sie das Simple Ransom Safe Backup Tool? ..... 2
- Das Simple Ransom Safe Backup Tool ..... 3
- Installation der SRSBT ..... 4
  - Voraussetzungen ..... 4
  - Das SRSBT De-Installieren ..... 4
- Die SRSBT-Funktionen ..... 4
  - Vorbereiten des externen mobilen Speichers ..... 4
  - Sicherungslisten und Ausschlussdateien ..... 4
    - Die Sicherungsliste ..... 4
    - Ausschlussdatei ..... 5
  - Dateien wiederherstellen ..... 6
  - Logs ..... 6
    - Verarbeitungslogs ..... 6
    - Sicherungslogs ..... 6
  - Sprachunterstützung ..... 6
  - Zeitangaben ..... 6
  - Sicherungsstrategien ..... 7
  - Alte Dateien ..... 7
- Die SRSBT-Anwendung ..... 7
  - Aufbau ..... 7
  - Kontext-Menü der Hauptdialogtextbox ..... 8
  - Die Funktionsknöpfe ..... 9
    - Laufwerk suchen ..... 9
    - Sichern starten ..... 9
  - Die Menü-Funktionen ..... 9

Menü „Datei“ .....	9
Menü „Hilfe“ .....	9
Soziales Hacking .....	9
Fehler, Fehlermeldung.....	10
Fehler im SRSBT.....	10
Warnung: Dateien haben dasselbe Datum, aber nicht die gleiche Größe .....	10
FAQ .....	10
Ich habe einen Virenschanner, schützt der mich nicht? .....	10
Ich sichere meine Daten in der Cloud, ist das nicht sicher? .....	11
Barrierefreiheit .....	11
Tastenkombinationen .....	11
Markenrechtliche Hinweise .....	11

## Aufgabe

Das Simple Ransom Safe Backup Tool, kurz SRSBT, dient dazu Kopien von Dateien eines Windows®-Rechners so zu verwahren, dass diese im Falle einer Ransomware-Attacke geschützt sind und bleiben.

### Was ist eine Ransomware-Attacke?

In einem typischen Ransomware-Szenario haben sich Hacker auf unterschiedlichste Weise von außen Zugriff auf ihren Computer verschafft. Nach der Installation einer Verschlüsselungssoftware (die Ransomware) werden sämtliche auf dem Computer befindlichen Dateien verschlüsselt, also für sie unlesbar gemacht. Um weiter arbeiten zu können verlangen die Hacker von ihnen einen, typischerweise sehr hohen, Betrag, nach deren Zahlung sie ihre Daten wieder entschlüsseln können – oder auch nicht.

### Wie schützt sie das Simple Ransom Safe Backup Tool?

Das SRSBT dient dazu, ihnen zu helfen, ihre Daten auf einen externen mobilen Speicher zu sichern. Die Idee ist, dass zum Zeitpunkt einer Attacke der externe mobile Speicher nicht an ihrem Rechner angeschlossen ist und die Daten damit der Verschlüsselung entgehen. Da dies nicht immer gewährleistet ist und da auch externe mobile Speicher von einem Ausfall betroffen sein können, empfiehlt es sich daher mindestens zwei externe mobile Speicher im Wechsel zu verwenden.

Wichtig ist es, dass die externen mobilen Speicher nur so lange wie nötig am Rechner angeschlossen sind. Deshalb sollten sie nach Verwendung des externen mobilen Speichers diesen immer sofort vom Rechner trennen!

***Sollten sie gehackt worden sein, schließen sie ihren externen mobilen Speicher nicht mehr an den Rechner an, bis sie die Bedrohung bereinigt haben!***

Die mit Hilfe des SRSBT gesicherten Daten dienen natürlich auch als ganz normales Backup.

Das Wort „Simple“ weist darauf hin, dass diese Lösung eine einfache und daher nicht perfekte Lösung zur Sicherung ihrer Daten ist.

Sie sollten in jedem Fall sich nicht allein auf diese Lösung verlassen, sondern auch potente Virens Scanner im Einsatz haben.

Wenn sie auf der Suche nach einer professionellen Lösung zur Sicherung ihrer Daten sind, dann schauen sie sich das Ransom Safe Backup System an: <https://www.qa-navigation.com/rsbs>.

## Das Simple Ransom Safe Backup Tool

Das SRSBT ist ein einfaches Programm mit einer grafischen Oberfläche. Die Arbeit mit dem SRSBT teilt sich in zwei Teile:

1. Vorbereitung der Sicherung
2. Durchführung der Sicherung

Bei der Vorbereitung der Sicherung werden mit Hilfe des SRSBT Sicherungs- und Ausschlusslisten erstellt, die später zur Steuerung der Sicherung dienen.

Die Sicherungs- und Ausschlusslisten dienen dazu, das Volumen und die Laufzeit der Sicherung zu begrenzen.

Im Verlauf der Sicherung stellt das SRSBT fest, ob die zu sichernde Datei bereits gesichert wurde und überspringt ggf. die Sicherung.

Alle Aktivitäten des SRSBT werden ausführlich erläutert und in verschiedenen Logs gesichert.

Sind die Sicherungs- und Ausschlusslisten erst einmal erstellt, erübrigt sich dieser Schritt bei allen weiteren Sicherungsläufen. Natürlich lassen sich die Sicherungs- und Ausschlusslisten jederzeit anpassen.

## Installation der SRSBT

Die Installation der SRSBT ist simpel: kopieren sie die ausführbare Datei „SRSBT.exe“ zusammen mit dieser Dokumentation an eine geeignete Stelle. Ggf. legen sie einen Schnellzugriff auf dem Desktop und/oder der Menüleiste an.

### Voraussetzungen

Das SRSBT wurde für Windows® 11 entwickelt.

### Das SRSBT De-Installieren

Sollten sie das SRSBT von ihren Systemen tilgen wollen, ist dies einfach zu bewerkstelligen, indem sie alle im Zusammenhang mit dem SRSBT stehenden Dateien löschen.

## Die SRSBT-Funktionen

### Vorbereiten des externen mobilen Speichers

Nachdem sie den externen mobilen Speicher angeschlossen haben, wählen sie den Button „Laufwerk suchen“. Anschließend wird eine Liste aller gefundenen externen Laufwerke angezeigt, inklusive der technischen Daten. Wählen sie das Laufwerk, das sie verwenden wollen.

Sollte der externe mobile Speicher noch nicht vorbereitet sein, wird ihnen angeboten, die notwendigen Dateien zu installieren.

Nachdem eine Installation vorgefunden wurde, wird der Button „Sichern starten“ freigeschaltet.

### Sicherungslisten und Ausschlussdateien

#### Die Sicherungsliste

Das SRSBT-Programm verarbeitet die auf dem Sicherungslaufwerk vorhandene Sicherungsliste SRSBTpaths.lst.

In der Sicherungsliste wird festgehalten, welche Pfade nach zu sichernden Dateien durchsucht wird.

Anhand dieser Liste durchläuft das SRSBT-Programm die Pfade ihres Rechners und sichert alle Dateien, die auf dem Weg liegen.

Einträge in der Sicherungsliste, die nicht als Pfad identifiziert werden, werden als Datei behandelt.

Zeilen, die mit einem „#“ beginnen werden als Kommentar ignoriert.

Alle Einträge müssen den vollständigen Pfad ab dem Punkt, wo gestartet werden soll, beinhalten und mit dem Laufwerksbuchstaben beginnen.

Es besteht die Möglichkeit sog. Wildcards (\*) zu verwenden. So bewirkt der Eintrag

*D:\Dev\Java\MeinProjekt\\*.java*

dass alle Pfade unterhalb von D:\Dev\Java\MeinProjekt durchlaufen werden und die dort gefundenen Dateien, die auf .java enden, gesichert werden.

Wildcards werden für Pfade nicht unterstützt.

Die Sicherung von Dateien direkt aus Cloud-Speichern wird z.Zt. nicht unterstützt. Um solche Dateien zu sichern binden sie den Cloud-Speicher als lokales Laufwerk in den Datei-Explorer ein.

Die Sicherungsliste findet sich auf dem Wurzelpfad des externen mobilen Speichers, z.B. „D:\SRSTpaths.lst“. Sie können sie kopieren, aber sie darf nicht gelöscht oder verschoben werden.

## Ausschlussdatei

Es kann, für jeden Pfad separat, eine Ausschlussdatei mit dem Namen ignore.srsb angelegt werden. Alle darin gefundenen Einträge werden herangezogen, um Dateien und/oder Pfade von der Sicherung auszuschließen.

Dabei wird geschaut, ob der angegebene Text Teil des Datei- oder Pfadnamens ist.

Bei der Verwendung von Wildcards („\*“) auf die resultierende Filterung achten. Sie kann unter Umständen zu großzügig sein.

Es können auch Pfade ausgeschlossen werden. „\bin“ bewirkt, dass alle Pfade, die dem Muster \*\bin entsprechen, ignoriert werden, ab dem aktuellen Verzeichnis.

**Wichtig:** wenn sie einen Pfad meinen, muss der Eintrag mit einem „\“ oder „/“ beginnen und enden!

Die spezifizierten Ausschlüsse gelten für alle unter dem aktuellen Pfad befindlichen Pfade. Weitere Ausschlüsse aus weiteren Ausschlussdateien in den Unterverzeichnissen werden akkumuliert.

Beachten sie bitte: auch versteckte Dateien werden gesichert. Sofern sie diese nicht mitgesichert haben wollen, müssen sie für sie entsprechende Muster in der Ausschlussdatei aufnehmen.

## *ignoreGlobal.srsb*

Die mit der Installation bereit gestellte *ignoreGlobal.srsb* beinhaltet empfohlene Filter für temporäre Dateien und Dateien, die anderweitig wiederherstellbar sind.

Die Liste kann den eigenen Bedürfnissen angepasst werden.

## Dateien wiederherstellen

Die gesicherten Dateien werden auf dem externen mobilen Speicher im Pfad „SRSBTbak“ hinterlegt, mit dem Pfad in dem sie gefunden wurden als Unterpfad, wobei das Laufwerk ohne „:“ inkludiert ist. So können sie die Dateien einzeln oder als komplette Datei-Bäume wieder zurückkopieren.

## Logs

### Verarbeitungslogs

Die Verarbeitung und etwaige Fehler führt das SRSBT im Log „SRSBT.log“ im Wurzelfeld des externen mobilen Speichers. In dem Log werden nur besondere Ereignisse ausgeführt. Z.B. das erfolgreiche Sichern einer Datei wird darin nicht erwähnt.

### Sicherungslogs

Die Liste erfolgreich gesicherter Dateien werden in einem separaten Log im Verzeichnis „SRSBTbak“ gespeichert, wobei für jeden Sicherungslauf eine Datei mit einem Namen der Form „SRSBT<yyyyMMddHHmmss>.log“ angelegt wird. Die Datei enthält u.a. die mit einem Zeitstempel versehene Liste der Dateien, die erfolgreich gesichert werden konnten, wobei auch die Dateien aufgeführt werden, die nicht kopiert wurden, da sie sich nicht geändert haben, mit einem entsprechenden Hinweis.

Da für jede Sicherung ein solches Log angelegt wird, empfiehlt es sich von Zeit zu Zeit einige der alten Logs zu löschen.

## Sprachunterstützung

Die SRSBT-Werkzeuge bemühen sich in ihren Dialogen die Sprache des Hostsystem anzubieten, wobei „Englisch (US)“ als Standardsprache gewählt wird, sollte die Sprache nicht erkannt oder unterstützt werden.

## Zeitangaben

Zeitangaben in den Logs und Meldungen erfolgen im Format JJJMMT-hh:mm:ss mit

- JJJ: Jahr
- MM: Monat
- TT: Tag
- hh: Stunde

- mm: Minute
- ss: Sekunde

## Sicherungsstrategien

Um die Laufzeit des SRSBT nicht unnötig hoch werden zu lassen und die Kapazitäten des externen mobilen Speichers nicht zu erschöpfen, sollten nur die Dateien gesichert werden, die nicht per Installation nach einer Ransomware-Attacke wiederhergestellt werden können, also vor allem diejenigen, die sich aus ihrer Arbeit ergeben.

Je nach ihrem Schutzbedürfnis sollten sie entscheiden, wie oft sie einen Sicherungslauf durchführen wollen. Einmal am Tag ist empfohlen.

## Alte Dateien

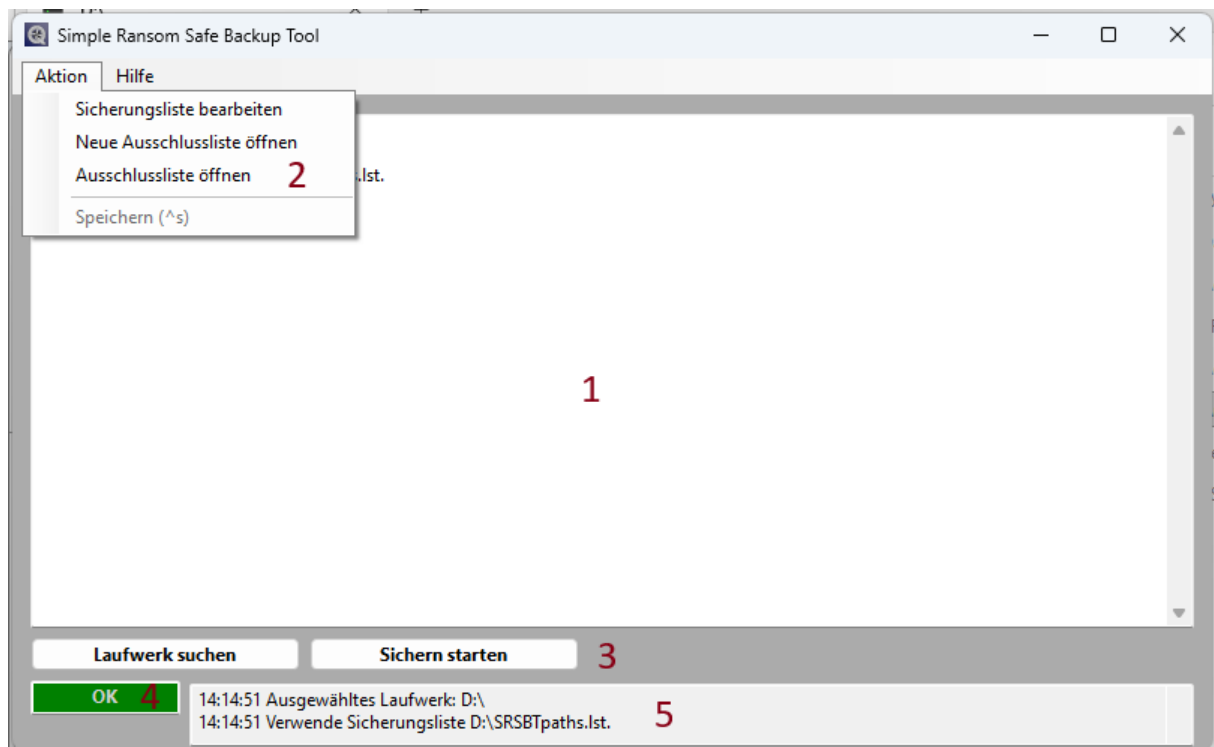
Existierende Dateien werden niemals gelöscht, nur Gleichnamige überschrieben. Es empfiehlt es sich die Sicherungslogs oder Sicherungslisten als Schnappschüsse zu sichern, wenn sich die Liste der gesicherten Dateien ändern.

Wenn sie einen bestimmten Stand sichern wollen, können sie einfach den Pfad SRSBTbak auf dem externen mobilen Speicher umbenennen und die Sicherung erneut laufen lassen.

## Die SRSBT-Anwendung

### Aufbau

Der SRSBT-Klient verfügt über ein Hauptdialogtextbox (1), Funktionsmenüs (2), Funktionsknöpfe (3), ein Status-Icon (4) und eine Log-Textbox (5).



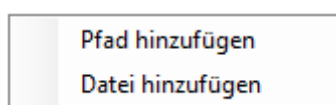
In der Hauptdialogtextbox werden entweder die in Arbeit befindlichen Dateien angezeigt oder die detaillierten Ausgaben einer Aktion angezeigt. Die Textbox ändert ihre Hintergrundfarbe zu Gelb, wenn der Inhalt einer Datei geändert wurde, um anzuzeigen, dass die Änderung gesichert werden muss. Nach dem Sichern der Datei wechselt die Textbox ihre Hintergrundfarbe wieder zurück zum Standard.

Das Status-Icon wechselt seine Farbe und Anzeige je Status der Verarbeitung von Grün/OK zu Gelb/In Arbeit und zurück. Im Falle eines Fehlers wechselt das Icon zu Rot/Fehler.

In der Log-Textbox werden die zuletzt in der Sitzung getätigten Aktionen festgehalten. Die Log-Textbox ist scrollbar.

## Kontext-Menü der Hauptdialogtextbox

Die Hauptdialogtextbox verfügt über ein Kontext-Menü, das mit Hilfe der rechten Maustaste aktiviert werden kann. Das Menü erscheint nur bei der Bearbeitung einer Datei.



- „Pfad hinzufügen“ ermöglicht es einer Sicherungsliste einen Pfad per Dialog hinzuzufügen.
- „Datei hinzufügen“ ermöglicht es einer Sicherungsliste eine Datei per Dialog hinzuzufügen.

## Die Funktionsknöpfe

### Laufwerk suchen

„Laufwerk suchen“ stößt die Suche nach externen mobilen Speichern an.

### Sichern starten

„Sichern starten“ startet die Sicherung der Daten anhand der Sicherungsliste.

## Die Menü-Funktionen

### Menü „Datei“

#### *Sicherungsliste bearbeiten*

Mit dieser Funktion lässt sich die Sicherungsliste SRSBTpaths.lst zur Bearbeitung öffnen.

#### *Neue Ausschlussliste öffnen*

„Neue Ausschlussliste öffnen“ öffnet einen Dialog zur Pfadauswahl. Im ausgewählten Pfad wird anschließend eine Ausschlussdatei angelegt und zur Bearbeitung geöffnet.

#### *Ausschlussliste öffnen*

„Ausschlussliste öffnen“ öffnet einen Dialog zur Pfadauswahl. Es wird die in dem Pfad vorhandene Ausschlussdatei ignore.srsb geöffnet. Sollte keine Ausschlussdatei vorliegen, wird diese angelegt.

#### *Speichern*

„Speichern“ speichert die an einer Datei gemachten Änderungen.

### Menü „Hilfe“

#### *Hilfe*

„Hilfe“ öffnet die Dokumentation zum SRSBT.

#### *Über ...*

„Über“ zeigt Informationen zum SRSBT und dessen Hersteller an.

## Soziales Hacking

**Wichtig!** Wir als Hersteller des SRSBT werden sie niemals per E-Mail oder Telefon zu Informationen ihres Rechners, ihrer SRSBT -Installation oder sonstiges Fragen, vor allem nicht nach Passwörtern, kontaktieren! Auch werden wird ihnen ungefragt keine Updates schicken; höchstens die Information, dass ein Update vorliegt, aber ohne Download-Link! Betrachten sie jeden solcher Versuche als Soziale-Hacking-Attacke. Wir werden höchsten bitten sich auf unserer Webseite zu informieren.

Mistrauen sie jedem einer Email beigefügten Link oder Links aus anderen Quellen. Am besten sie navigieren eigenhändig zu unserer Website.

## Fehler, Fehlermeldung

Bei jeder Aktion werden Fehler immer auch in der jeweiligen Log-Datei festgehalten, ggf. mit größerer Detailtiefe.

Prüfen sie regelmäßig das Log auf Unstimmigkeiten!

Führen sie regelmäßig Wiederherstellungsläufe zur Probe durch!

## Fehler im SRSBT

Das SRSBT wurde mit größter Aufmerksamkeit auf Robustheit und Stabilität entwickelt. Schon während der Entwicklung wurde auf eine möglichst niedrige Fehlerquote geachtet und die verbliebenen Fehler wurden mit Hilfe intensiver Tests weiter reduziert. Trotzdem, das SRSBT ist Software und Software wird niemals 100% fehlerfrei sein. Verlassen sie sich deshalb nicht blind auf das SRSBT sondern beobachten sie seine Arbeit kritisch, damit das SRSBT sie nicht im Stich lässt, wenn sie es brauchen.

Gleichermaßen gilt: das SRSBT kann ihre Daten nur dann gut beschützen, wenn sie die Datensicherung mit dem SRSBT mit entsprechender Sorgfalt behandeln.

## Warnung: Dateien haben dasselbe Datum, aber nicht die gleiche Größe

Diese Warnung kann ein Hinweis sein, dass ihre Dateien bereits verändert wurden, während die Hacker clever genug waren, das Datum der Datei beizubehalten.

In diesem Fall wird die Datei nicht gesichert. Prüfen sie die Dateien und unternehmen sie entsprechende Maßnahmen.

## FAQ

### Ich habe einen Virenschanner, schützt der mich nicht?

Der Schutz durch Virenschanner beruht darauf, dass die sog. Malware auf Grund ihres bereits bekannten Codes oder ihres Verhaltens erkannt wird. Der Schutz durch Virenschanner wird durch Hacker unterlaufen, in dem sie immer neue Varianten ihrer Viren in Umlauf bringen, die die Virenschanner nicht kennen.

Außerdem schützen Virenschanner nicht vor sogenanntem Sozial-Hacking, bei dem ein Benutzer in gutem Glauben den Hacker selbst Zutritt zu ihren Rechnern verschafft.

Mit dem SRSBT werden ein Virens Scanner oder andere Schutzmaßnahmen nicht überflüssig. Vielmehr ergänzen sich diese Maßnahmen, bei der das SRSBT eine letzte Bastion bildet.

## Ich sichere meine Daten in der Cloud, ist das nicht sicher?

Auch Daten in der Cloud können überschrieben oder gelöscht werden, mit den Rechten des Benutzers, was die Hacker ausnutzen. Darüber hinaus unterlaufen auch Cloud-Speicher Datenverlust und Cyber-Attacken. Im Gegenteil: Cloud-Server sind für Hacker ein viel lohnenswerteres Ziel als individuelle Rechner, weil der Schaden größer ist und damit das Erpressungspotential.

## Barrierefreiheit

Es wurde darauf geachtet das SRSBT und seine Dokumentation barrierefrei zu gestalten.

Es gibt keine grafischen Elemente, die Informationen ohne textuelle Unterstützung transportieren. Wo Bilder vorkommen, dienen diese ausschließlich dazu, das Beschriebene nochmals grafisch zu präsentieren.

Der SRSBT-Klient ist ohne Maus bedienbar; alle Elemente sind mit Hilfe der Standard-Tastenkombinationen erreichbar.

Für Elemente, die nicht selbsterklärend sind, wurden Alternativtexte hinterlegt.

## Tastenkombinationen

- ALT + Buchstabe: Öffnen eines der Hauptmenüs.
- Umschalttaste + F10: Aufruf des Kontextmenüs.

Innerhalb aller Menüs können die Kommandos mit ihrem Anfangsbuchstaben angesprungen oder ausgelöst werden.

Alle Elemente sind per Tab-Sprung und Pfeil-Operationen erreichbar.

## Markenrechtliche Hinweise

.NET: Das Microsoft.NET-Logo ist ein eingetragenes Markenzeichen der Microsoft Corporation in den Vereinigten Staaten von Amerika und/oder anderen Ländern.

Microsoft®, Windows® und das Windows-Logo sind eingetragene Markenzeichen der Microsoft Corporation in den Vereinigten Staaten von Amerika und/oder anderen Ländern.