

# OPSEC

## Inhaltsverzeichnis

- [I. Warum OPSEC im Prepping wichtig ist](#)
- [II. Schutz der persönlichen Informationen](#)
- [III. Verschleierung und Desinformation als Mittel der OPSEC](#)
- [IV. Sichere Kommunikation im Prepping-Umfeld](#)
- [V. Schutz des Vorratsorts durch OPSEC](#)
- [VI. Auswahl und Aufbewahrung von Dokumenten](#)
- [VII. Risikobewertung und regelmäßige Überprüfung der OPSEC-Maßnahmen](#)
- [VIII. OPSEC und die Bedeutung der Anonymität](#)

Im Bereich des Preppings spielt OPSEC (Operational Security oder Operationssicherheit) eine zentrale Rolle. OPSEC, ein Konzept aus dem Militär, beschreibt Methoden und Strategien, um kritische Informationen zu schützen, die den eigenen Sicherheitsmaßnahmen schaden könnten, wenn sie in die falschen Hände geraten. Im Kontext des Preppings geht es darum, seine Vorbereitungen, Vorräte, Ausrüstungen und Pläne bestmöglich zu verbergen und sich selbst und seine Familie vor potenziellen Risiken zu schützen.

### **I. Warum OPSEC im Prepping wichtig ist**

Viele Menschen im Bereich des Preppings bemühen sich um [Autarkie](#) und Unabhängigkeit, insbesondere in Krisensituationen. Dabei kann es um Themen wie [Notvorräte](#), medizinische Versorgung und Selbstverteidigung gehen. Ohne adäquate OPSEC-Maßnahmen könnte das Wissen über diese Vorbereitungen jedoch Begehrlichkeiten bei Dritten wecken, insbesondere in Notlagen. Die Gefahr, dass Außenstehende versuchen, sich im Krisenfall Zugang zu den Ressourcen eines Preppers zu verschaffen, ist real und sollte durch eine konsequente OPSEC minimiert werden.

### **II. Schutz der persönlichen Informationen**

Einer der wichtigsten Aspekte der OPSEC ist der Schutz der persönlichen Informationen. Zu diesen zählen Details über den eigenen Wohnort, die Lagerung von Vorräten und die eingesetzten Sicherheitsmaßnahmen. Jeder Hinweis darauf, dass jemand über Vorräte und Wissen verfügt, kann Außenstehende anziehen und potenziell gefährden. Es ist daher ratsam, persönliche Informationen mit Bedacht zu teilen und vorsichtig mit Informationen umzugehen, die durch soziale Medien, Gespräche oder Einkäufe preisgegeben werden könnten.

- Datenmengen minimieren: Nur notwendige Informationen auf Plattformen und Social Media preisgeben. Alles, was nicht unbedingt geteilt werden muss, sollte diskret bleiben.
- Social Media bewusst nutzen: Verzichten Sie auf Details, die Rückschlüsse auf Vorratsmengen, Lagerorte oder Sicherheitsstrategien zulassen.
- Netzwerke diskret halten: Auch in privaten Netzwerken wie Foren oder Gruppen sollte immer darauf geachtet werden, nur mit absolutem Vertrauen Informationen auszutauschen.

### **III. Verschleierung und Desinformation als Mittel der OPSEC**

Ein bewährter OPSEC-Ansatz ist die gezielte Verschleierung und Desinformation. Statt detailliert zu erläutern, wie viele Vorräte vorhanden sind oder welche Vorbereitungen getroffen wurden, kann es hilfreich sein, absichtlich vage oder falsche Informationen zu streuen.

- Geringe Mengen angeben: Sprechen Sie im Bekanntenkreis eher von kleinen Vorräten, um keine Begehrlichkeiten zu wecken. Die Erwähnung von „ein paar Dosen“ oder „einer Notfalltasche“ wirkt weniger interessant als detaillierte Informationen.
- Tarnung nutzen: Wenn Sie Vorräte anlegen, sollten diese so gelagert werden, dass sie von außen schwer zugänglich und nicht auf den ersten Blick zu sehen sind. Versteckte Vorratsräume oder geschickt versteckte Notfallvorräte können zusätzlich schützen.

#### **IV. Sichere Kommunikation im Prepping-Umfeld**

Eine weitere kritische Komponente der OPSEC im Prepping ist die Kommunikationssicherheit. Gerade bei Treffen oder beim Austausch über Vorsorgemaßnahmen ist es wichtig, dass diese Kommunikation nicht ohne Weiteres abgefangen oder missbraucht werden kann.

- Verschlüsselte Kommunikation: Bei der Kommunikation über das Internet sollten verschlüsselte Nachrichten-Apps wie Signal oder Threema genutzt werden, um den Austausch über Pläne und Ressourcen zu schützen.
- Sichere Telefonie: Auch beim Telefonieren ist darauf zu achten, möglichst auf sichere Netze zu setzen. Besonders vertrauliche Informationen sollten besser persönlich besprochen werden.

#### **V. Schutz des Vorratsorts durch OPSEC**

Ein zentrales Ziel der OPSEC ist es, den Vorratsort nicht nur physisch, sondern auch durch [Verschleierungstaktiken](#) zu schützen. Dies schließt alle Vorbereitungen ein, die notwendig sind, um Lebensmittel, Wasser und andere Ressourcen langfristig unentdeckt und sicher aufzubewahren.

- Geheime Vorratsräume: Das Anlegen von versteckten Lagerräumen im Keller oder hinter falschen Wänden kann einen erheblichen Schutz bieten. Diese Vorratsräume sollten möglichst nur von den unmittelbar Beteiligten bekannt sein.
- Tarnung in der Umgebung: Der Standort der Vorratsräume sollte so gewählt werden, dass er weder auffällig noch leicht zugänglich ist. Ein Lager im Hinterzimmer oder in einem nicht genutzten Schuppen kann oft unbemerkt bleiben, wenn es durch Alltagsgegenstände wie Regale, Kisten oder andere Möbelstücke getarnt wird.
- Ungewöhnliche Vorratsverstecke: Auch im Garten oder auf dem Grundstück können Vorräte sicher verwahrt werden. Unterirdische Lagerstätten, mit Tarnmaterial abgedeckt, können ebenfalls eine hohe Sicherheit bieten.

#### **VI. Auswahl und Aufbewahrung von Dokumenten**

Ein häufig unterschätzter Bereich der OPSEC betrifft wichtige Dokumente. Jeder Prepping-Plan sollte eine Sammlung essenzieller Dokumente wie Ausweise, Versicherungsnachweise und medizinische Informationen enthalten. Diese Dokumente müssen jedoch besonders geschützt und sicher aufbewahrt werden.

- Dokumentensicherung in wasserdichten Behältern: Es ist ratsam, Dokumente in feuerfesten und wasserdichten Boxen zu lagern, um sie vor Umwelteinflüssen und äußeren Schäden zu schützen.
- Backup-Optionen: Digitale Kopien dieser Dokumente können zusätzlich auf verschlüsselten USB-Sticks oder sicheren Cloud-Speicherlösungen hinterlegt werden. Dabei ist wichtig, dass der Zugang durch starke Passwörter und Authentifizierungsmaßnahmen geschützt wird.

#### **VII. Risikobewertung und regelmäßige Überprüfung der OPSEC-Maßnahmen**

Die kontinuierliche Risikobewertung und Anpassung der OPSEC-Strategien ist ein wichtiger Bestandteil der Sicherheit im Prepping. Die Bedrohungslage und die eigenen Sicherheitsmaßnahmen können sich mit der Zeit ändern, weshalb eine regelmäßige Überprüfung und Anpassung der Maßnahmen notwendig ist.

- Erneute Risikoeinschätzung: Die regelmäßige Einschätzung, wie sich die eigene Lage entwickelt hat, und Anpassungen der OPSEC-Maßnahmen sind entscheidend. Überprüfen Sie, ob bisher geteilte Informationen problematisch werden könnten.
- Neue Entwicklungen beobachten: Auch gesellschaftliche und politische Entwicklungen sollten in die OPSEC-Strategien einbezogen werden. Eine erhöhte Sensibilität für Sicherheitsfragen und das Bewusstsein für eventuelle Schwachstellen kann langfristig schützen.
- Flexibilität: Eine flexible OPSEC-Strategie ermöglicht es, im Ernstfall schnell und effektiv zu reagieren und sich vor potenziellen Bedrohungen zu schützen.

## VIII. OPSEC und die Bedeutung der Anonymität

Im Bereich des Preppings kann es sinnvoll sein, auf Anonymität zu setzen. Dazu zählt, dass so wenig wie möglich über die eigenen Vorbereitungen und Vorräte preisgegeben wird. Auch in Gesprächen und Netzwerken ist es ratsam, auf ein Minimum an Informationen zu setzen und möglichst anonym zu bleiben.

- Anonyme Einkaufsstrategien: Große Mengen an Vorräten und spezifische [Prepper](#)-Ausrüstung sollten unauffällig und idealerweise anonym gekauft werden. Dies kann durch den Einkauf in bar oder über verschiedene Standorte und Geschäfte verteilt geschehen.
- Nutzung von Pseudonymen: In Foren und bei Online-Einkäufen kann die Verwendung eines Pseudonyms zur Anonymität beitragen und die Rückverfolgbarkeit erschweren.
- Diskrete Lagerung: Ein unauffälliges Erscheinungsbild der Vorratsorte und keine offensichtliche Ausrüstung können ebenfalls dazu beitragen, ungewollte Aufmerksamkeit zu vermeiden.