



# OTScan

OT-Netzwerk-Scanner für industrielle Umgebungen · Version 2.0.1

## BENUTZERHANDBUCH

Installation, Lizenz, Bedienung und alle Funktionen

---

**Version 2.0.1** · Stand 28.09.2026

Herausgeber: Jörg Hansel, HanselCraft · [hanselcraft.de](https://hanselcraft.de)

# Inhaltsverzeichnis

|                                                        |    |
|--------------------------------------------------------|----|
| <b>1 Einleitung und Zweck</b>                          | 3  |
| <b>2 Sicherheitshinweise vor dem ersten Scan</b>       | 3  |
| <b>3 Systemvoraussetzungen</b>                         | 4  |
| <b>4 Installation</b>                                  | 5  |
| 4.1 Lieferumfang                                       | 5  |
| 4.2 Windows: Nmap und Npcap installieren               | 5  |
| 4.3 Windows: Setup (empfohlen)                         | 5  |
| 4.4 Windows: portable Programmdatei                    | 5  |
| 4.5 Linux                                              | 6  |
| 4.6 Erster Start                                       | 6  |
| 4.7 Update                                             | 6  |
| 4.8 Deinstallation                                     | 6  |
| 4.9 Datenablage                                        | 7  |
| <b>5 Testphase und Lizenz</b>                          | 7  |
| 5.1 Testphase (3 Tage)                                 | 7  |
| 5.2 Lizenz aktivieren                                  | 7  |
| 5.3 Online-Aktivierung: welche Daten übertragen werden | 8  |
| 5.4 Aktivierung ohne Internet                          | 8  |
| <b>6 Die Oberfläche</b>                                | 8  |
| <b>7 Netzwerke verwalten</b>                           | 9  |
| <b>8 Scan-Profile und Portsets</b>                     | 9  |
| 8.1 Die Standardprofile                                | 9  |
| 8.2 Portsets                                           | 10 |
| 8.3 Eigene Profile                                     | 11 |
| <b>9 Scan durchführen (Run)</b>                        | 11 |
| <b>10 NSE-Skripte</b>                                  | 11 |
| <b>11 Risiko-Ampel</b>                                 | 12 |
| 11.1 Gewichtung                                        | 12 |
| 11.2 Ampelregeln                                       | 12 |
| <b>12 Berichte</b>                                     | 13 |
| <b>13 Weitere Funktionen</b>                           | 13 |
| 13.1 History und Delta                                 | 13 |
| 13.2 Inventar-Abgleich (CMDB)                          | 13 |
| 13.3 Hersteller/OS-Regeln                              | 13 |
| 13.4 Splunk-DB (Firewall-Kommunikation)                | 14 |
| <b>14 Branding: eigenes Logo im Report</b>             | 14 |
| <b>15 Kommandozeilen- und Headless-Modus</b>           | 14 |
| <b>16 Fehlerbehebung</b>                               | 15 |
| <b>17 Rechtliches und Datenschutz</b>                  | 15 |

# 1 Einleitung und Zweck

OTScan ist ein Inventarisierungs- und Risiko-Scanner für OT- und ICS-Netze (Operational Technology, industrielle Steuerungs- und Gebäudeautomationsnetze). Das Programm steuert die frei verfügbare Scan-Engine **Nmap** und wertet deren Ergebnisse aus:

- Es erkennt Geräte in den gewählten Netzen und ordnet sie Geräteklassen zu (z. B. SPS, HMI, Energiemessgerät, Netzwerkkomponente, Gebäudeautomation).
- Es fragt über mitgelieferte NSE-Skripte herstellertypische Identitätsdaten ab (Modell, Firmware, Seriennummer, soweit das Gerät sie liefert).
- Es bewertet offene Dienste mit einer **Risiko-Ampel** (ROT / GELB / GRÜN / INFO), die OT-Steuerprotokolle und unsichere IT-Protokolle gewichtet.
- Es erzeugt Berichte als **Excel**, **PDF** und **PowerPoint**, speichert jeden Lauf in einer lokalen Datenbank und zeigt Veränderungen zwischen zwei Scans (Delta).

OTScan sendet **keine Schreib-, Steuer- oder Start/Stopp-Befehle** an Geräte. Ein aktiver Scan ist trotzdem nicht „rückwirkungsfrei“: Jeder Scan erzeugt Netzlast und Verbindungsversuche, auf die sehr alte oder empfindliche Steuerungen reagieren können. Deshalb gibt es schonende Profile, eine Bestätigungsabfrage vor jedem Scan und die Hinweise in Kapitel 2.

Dieses Handbuch gilt für **OTScan 2.0.1** (Windows und Linux). Ab dieser Version wird OTScan als fertige Programmdatei geliefert; eine Python-Installation oder Offline-Pakete sind nicht mehr nötig.

## 2 Sicherheitshinweise vor dem ersten Scan

**Nur mit Genehmigung scannen.** Setzen Sie OTScan ausschließlich in Netzen ein, die Ihnen gehören oder für die eine ausdrückliche, möglichst schriftliche Genehmigung des Netzbetreibers vorliegt (Umfang, IP-Bereiche, Zeitfenster, Ansprechpartner). Das Scannen fremder Netze ohne Erlaubnis kann strafbar sein und Schadenersatzansprüche auslösen.

**Steuerungen schonen.** Beginnen Sie in Produktionsnetzen mit dem Profil „**Discovery v2 (saubere Ports, schonend)**“ und einem kleinen Adressbereich. Tiefenscans mit Betriebssystemerkennung, UDP und NSE-Skripten (insbesondere **FORCE**) nur in abgestimmten Wartungsfenstern und mit Rückfallplan. Empfindliche Alt-SPSen können auf ungewöhnliche Pakete mit Verbindungsabbrüchen oder im Extremfall mit einem Stopp reagieren.

Vor jedem Scan zeigt OTScan das Fenster „**Warnung – OT-Netzwerkscan**“. Es nennt Netz, Profil, Portset und den Rechte-Status und verlangt drei Bestätigungen: Freigabe liegt vor, schonendes Profil gewählt, Zeitfenster abgestimmt. Erst dann startet der Scan.

Die Ergebnisse (Gerätekategorie, Ampel) sind Hilfsindikatoren und ersetzen keine fachliche Bewertung. Näheres regelt die Datei `HAFTUNG_UND_NUTZUNG.txt` im Paket.

### 3 Systemvoraussetzungen

| Komponente        | Windows                                                                                                     | Linux                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssystem    | Windows 10 (ab Version 1809) oder Windows 11, 64 Bit (x64)                                                  | x86_64 mit <b>glibc 2.31 oder neuer</b> : z. B. Debian 11, Ubuntu 20.04, Linux Mint 20 und neuer. Getestet: Debian 11, Ubuntu 22.04, Ubuntu 24.04. <b>Nicht</b> lauffähig: RHEL/Rocky 8, CentOS 7 |
| Python            | nicht nötig (in der Programmdatei enthalten)                                                                | nicht nötig (Python und Tk sind enthalten)                                                                                                                                                        |
| Nmap              | <b>separat installieren</b> von nmap.org (Windows-Installer), empfohlen aktuelle Version; getestet mit 7.99 | <b>separat installieren</b> über die Paketverwaltung (sudo apt install nmap, Fedora: sudo dnf install nmap); getestet mit 7.80 und 7.94                                                           |
| Paketaufzeichnung | <b>Npcap</b> (wird vom Nmap-Installer mitinstalliert)                                                       | im System enthalten                                                                                                                                                                               |
| Rechte            | Administratorrechte für die Installation von Nmap/Npcap und für SYN-, UDP- und OS-Scans                     | <b>root</b> (über <b>sudo</b> ) für SYN-, UDP- und OS-Scans                                                                                                                                       |
| Oberfläche        | Bildschirm ab ca. 1280 × 800                                                                                | grafische Sitzung: X11 oder Wayland mit XWayland                                                                                                                                                  |
| Speicher          | ca. 150 MB für Programm und temporäres Entpacken, zusätzlich Platz für Reports                              | ca. 150 MB, zusätzlich Platz für Reports                                                                                                                                                          |
| Internet          | nur einmal für die Online-Aktivierung der Lizenz (optional, siehe Kapitel 5)                                | wie Windows                                                                                                                                                                                       |

**Nmap wird nicht mitgeliefert.** OTScan ruft das Programm `nmap` auf, das im Suchpfad (`PATH`) liegen muss. Der Windows-Installer von nmap.org trägt Nmap standardmäßig in den `PATH` ein.

Download-Adressen:

- Nmap für Windows (inkl. Npcap): <https://nmap.org/download.html>
- Npcap einzeln (falls separat nötig): <https://npcap.com/#download>

#### Hinweise zu den Administratorrechten (Windows):

- Nmap und Npcap installieren Sie einmalig mit Administratorrechten.
- Aktivieren Sie im Npcap-Installer die Option „**Restrict Npcap driver's access to Administrators only**“ nur, wenn OTScan ohnehin immer als Administrator gestartet wird.
- Profile mit SYN-, UDP- oder OS-Erkennung (`-sS`, `-sU`, `-O`) brauchen zur Laufzeit Administratorrechte. OTScan fragt beim Start, ob es mit Administratorrechten neu starten soll. Ohne Administratorrechte ist nur das Profil „Discovery v2“ (TCP-Connect-Scan) voll nutzbar.

## 4 Installation

### 4.1 Lieferumfang

| Paket                            | Inhalt                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OTScan_2.0.1_Windows.zip         | OTScan_Setup_v2.0.1.exe (Setup),<br>OTScan_v2.0.1.exe (portable Programmdatei),<br>nse_scripts\ (22 NSE-Skripte + 2 Bibliotheken zur Einsicht),<br>docs\ (Handbuch, NSE-Dokumentation, Schulungsunterlagen,<br>Methodik), Muster-Report\, LIESMICH.txt,<br>EULA.txt, HAFTUNG_UND_NUTZUNG.txt,<br>THIRD_PARTY_NOTICES.txt,<br>LICENSE_NPSL_Nmap.txt, PAKETINHALT.txt |
| OTScan_2.0.1_Linux_x86_64.tar.gz | Programmdatei OTScan, nse_scripts/, docs/ (dieses<br>Handbuch), LIESMICH.txt, CHANGELOG.txt, EULA.txt,<br>LICENSE.txt, HAFTUNG_UND_NUTZUNG.txt,<br>THIRD_PARTY_NOTICES.txt,<br>LICENSE_NPSL_Nmap.txt                                                                                                                                                                |

Die NSE-Skripte sind **in der Programmdatei eingebettet** und werden automatisch verwendet. Die Kopie im Ordner `nse_scripts` dient zur Einsicht und zur Erfüllung der Nmap-Lizenz; sie muss nicht in den Nmap-Ordner kopiert werden.

### 4.2 Windows: Nmap und Npcap installieren

1. Den aktuellen Nmap-Installer für Windows von [nmap.org](http://nmap.org) laden und mit Administratorrechten ausführen.
2. Im Installer die Komponente **Npcap** ausgewählt lassen und installieren.
3. Prüfen: Eingabeaufforderung öffnen und `nmap --version` eingeben. Es muss eine Versionsangabe erscheinen.

### 4.3 Windows: Setup (empfohlen)

1. Die ZIP-Datei vollständig entpacken (nicht aus der ZIP heraus starten).
2. OTScan\_Setup\_v2.0.1.exe starten. Das Setup benötigt **keine Administratorrechte**.
3. Lizenzbedingungen (EULA) und Nutzungshinweise bestätigen, optional eine Desktop-Verknüpfung wählen.

Das Setup installiert nach `%LOCALAPPDATA%\Programs\OTScan` und legt im Startmenü folgende Einträge an: „OTScan“, „OTScan (als Administrator für SYN/UDP/OS-Scans)“ (dort per Rechtsklick „Als Administrator ausführen“ wählen), „Benutzerhandbuch“ und „OTScan deinstallieren“. Ein vorhandenes OTScan 2.0.0 aus dem Setup wird dabei aktualisiert; Ihre Daten bleiben erhalten.

Windows SmartScreen kann beim ersten Start „Der Computer wurde durch Windows geschützt“ melden. Über **„Weitere Informationen → Trotzdem ausführen“** starten. Prüfen Sie vorher die SHA-256-Prüfsumme der Download-Datei (Datei `SHA256SUMS.txt` neben dem Download).

### 4.4 Windows: portable Programmdatei

OTScan\_v2.0.1.exe kann ohne Installation direkt gestartet werden, z. B. von einem USB-Stick oder aus einem beliebigen Ordner. Für SYN-, UDP- und OS-Scans per Rechtsklick **„Als Administrator ausführen“**. Der erste Start dauert einige Sekunden, weil die Programmdatei ihre Bestandteile in einen temporären Ordner entpackt.

## 4.5 Linux

```
tar xzf OTScan_2.0.1_Linux_x86_64.tar.gz
cd OTScan_2.0.1_Linux_x86_64
chmod +x OTScan
./OTScan          # Connect-Scans, Reports, Inventar
sudo ./OTScan     # SYN-/UDP-/OS-Scans und tiefe NSE-Scans
```

Die glibc-Version prüfen Sie mit `ldd --version`.

**Wayland (Standard ab Ubuntu 22.04):** Grafische Programme dürfen als `root` oft nicht auf den Bildschirm. Erscheint nach `sudo ./OTScan` kein Fenster (das Programm endet sofort ohne Meldung), einmal pro Sitzung ausführen: `xhost +SI:localuser:root` und OTScan erneut mit `sudo` starten.

Unter `sudo` gilt das Home-Verzeichnis von `root`: Testphase, Lizenz und Datenbank liegen dann getrennt von denen des normalen Benutzers.

## 4.6 Erster Start

1. **Startdialog (nur Windows ohne Administratorrechte):** „Ja“ startet OTScan mit Administratorrechten neu, „Nein“ startet ohne (nur Connect-Scans), „Abbrechen“ beendet.
2. Kurze Startanimation, danach das Hauptfenster. In der Titelseite stehen Version, Build und der Lizenzstatus, z. B. `OTScan 2.0.1 · Build 2.0.1-20260927 · Testversion – 3 Tag(e) übrig`.
3. Beim ersten Start legt OTScan seinen Datenordner, die Datenbank und die Standardprofile an.

## 4.7 Update

OTScan sucht nicht selbst nach Updates. Neue Versionen laden Sie manuell über den Download-Link Ihres Kaufs bzw. über [hanselcraft.de](https://hanselcraft.de).

- **Setup:** das neue Setup einfach ausführen; es aktualisiert die vorhandene Installation.
- **Portabel:** die alte Programmdatei durch die neue ersetzen.
- **Linux:** das neue Archiv entpacken und die neue Programmdatei starten.

Datenbank, Profile, Einstellungen und die Lizenz bleiben erhalten, da sie im Benutzerprofil liegen. Lizenzschlüssel aus Version 2.0.0 gelten weiter.

## 4.8 Deinstallation

- **Setup:** Windows-Einstellungen → Apps → „OTScan 2.0.1“ → Deinstallieren, oder Startmenü „OTScan deinstallieren“. Entfernt werden die Programmdateien und Verknüpfungen.
- **Portabel / Linux:** den Programmordner löschen.

Ihre Daten bleiben bei der Deinstallation erhalten. Wenn Sie OTScan vollständig entfernen möchten, löschen Sie zusätzlich die Datenordner aus Abschnitt 4.9 (vorher Reports und Datenbank sichern; die Lizenzdatei aufheben, falls Sie OTScan später wieder installieren).

## 4.9 Datenablage

| Inhalt                                                                                     | Windows                                                                                             | Linux                                        |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------|
| Programm (Setup)                                                                           | %LOCALAPPDATA%\Programs\OTScan                                                                      | Ordner, in den Sie das Archiv entpackt haben |
| Datenbank otscan.db, settings.json, Hersteller/OS-Regeln, branding_config.json, Protokolle | %APPDATA%\OTScan                                                                                    | ~/.local/share/OTScan                        |
| Eigene/aktualisierte NSE-Skripte (optional)                                                | %APPDATA%\OTScan\nse_scripts                                                                        | ~/.local/share/OTScan/nse_scripts            |
| Lizenz und Testphase                                                                       | %LOCALAPPDATA%\OTScan (license.dat, trial.dat) sowie ein kleiner Eintrag unter HKCU\Software\OTScan | ~/OTScan und ~/.config/otscan                |
| Scan-Ergebnisse und Reports                                                                | frei wählbar, Standard: Dokumente                                                                   | frei wählbar, Standard: ~/Documents          |

Scan-Ergebnisse verlassen Ihren Rechner nicht. OTScan enthält kein Tracking und keine Telemetrie.

## 5 Testphase und Lizenz

### 5.1 Testphase (3 Tage)

Nach dem ersten Start läuft eine **Testphase von 3 Tagen** mit vollem Funktionsumfang. Die verbleibenden Tage stehen in der Titelseite. Der Beginn der Testphase wird signiert an mehreren Stellen im Benutzerprofil gespeichert; das Löschen einzelner Dateien oder ein Zurückstellen der Uhr verlängert die Testphase nicht. Ein Wechsel des Netzwerkadapters (Docking, WLAN, VPN) oder des Rechnernamens beendet eine laufende Testphase **nicht**.

### 5.2 Lizenz aktivieren

Nach dem Kauf erhalten Sie einen Lizenzschlüssel (Text beginnend mit **OTSCAN-**). Sie können ihn **jederzeit** eingeben, auch während der Testphase:

1. In der Seitenleiste auf „**Lizenz eingeben...**“ klicken. (Nach Ablauf der Testphase erscheint das Fenster „**Testphase abgelaufen**“ beim Start automatisch.)
2. Lizenzschlüssel vollständig einfügen (Zeilenumbrüche und Leerzeichen werden ignoriert).
3. „**Aktivieren**“ klicken. Bei Erfolg erscheint „OTScan ist jetzt lizenziert“, die Titelseite zeigt „Lizenziert (Name)“ und der Button heißt dann „Lizenz (aktiv)...“.
4. Bei „Ungültiger oder abgelaufener Schlüssel“ den Schlüssel auf Vollständigkeit prüfen. „Später“ schließt das Fenster; die Testphase läuft weiter.

Die Lizenz wird im Benutzerprofil gespeichert (siehe 4.9). Wird OTScan unter einem **anderen Windows-Konto** gestartet (z. B. ein separates Administratorkonto bei der Rechteabfrage), gilt dessen eigenes Profil; dort muss der Schlüssel einmal erneut eingegeben werden. Unter Linux gilt dasselbe für **sudo** (Profil von **root**).

### 5.3 Online-Aktivierung: welche Daten übertragen werden

Die Gültigkeit des Schlüssels prüft OTScan **offline** anhand einer digitalen Signatur. Zusätzlich meldet OTScan die Aktivierung einmalig an den Lizenzserver von HanselCraft (Cloudflare Workers, Cloudflare Inc., USA). Übertragen werden per HTTPS:

- der **Lizenzschlüssel** – er enthält den Namen des Käufers und die Bestellnummer;
- eine **Geräte-ID**: ein nicht umkehrbarer SHA-256-Hashwert aus Rechnername und Netzwerkadresse (MAC) des Rechners;
- technisch bedingt Ihre **IP-Adresse** (sie wird nur kurzzeitig, höchstens etwa zwei Minuten, zur Begrenzung von Anfragen verwendet).

Der Server speichert zum Schlüssel (als Hashwert) die Geräte-ID, den Zeitpunkt der ersten und letzten Aktivierung und die Anzahl der Aktivierungen. Zweck: Nachweis der Lizenz und Erkennung von Missbrauch. Scan-Ergebnisse, Netzbereiche, Gerätelisten oder Reports werden **nicht** übertragen.

### 5.4 Aktivierung ohne Internet

Ist der Rechner offline (typisch für OT-Netze), funktioniert die Aktivierung trotzdem: Die Signaturprüfung erfolgt lokal, die Meldung an den Server entfällt dann ohne Fehlermeldung. Eine spätere Online-Verbindung ist nicht erforderlich.

## 6 Die Oberfläche

Links befindet sich die Seitenleiste, rechts die jeweilige Arbeitsfläche. Unten zeigt die Statusleiste Uhrzeit, letzten Scan und Version.

| Eintrag            | Funktion                                                                                                                       |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Netzwerke          | Zielnetze anlegen, aus TXT/CSV oder Excel importieren, löschen                                                                 |
| Scan-Typen         | Scan-Profile und Portsets ansehen, anlegen, duplizieren, ändern; Hilfe zu Parametern, NSE-Skripten, Portsets und ICS/OT-Wissen |
| Run                | Scan zusammenstellen, Export wählen, Warteschlange starten, Reports neu erzeugen                                               |
| History            | frühere Scans, Reports und Delta-Vergleiche                                                                                    |
| Inventar-Abgleich  | Abgleich der Scan-Ergebnisse mit einem Soll-Inventar (CMDB-Excel)                                                              |
| Hersteller/OS      | eigene Regeln zur Korrektur von Herstellernamen und Betriebssystem                                                             |
| Splunk-DB (n)      | Firewall-Kommunikation je Netz aus einem Splunk-XML-Export hinterlegen; n = Anzahl der Netze mit Daten                         |
| Lizenz eingeben... | Lizenzschlüssel eingeben (auch während der Testphase); nach der Aktivierung „Lizenz (aktiv)...“                                |

Die Planung wiederkehrender Scans (Scheduler) ist in Version 2.0.1 deaktiviert; OTScan scannt nur nach manuellem Start (oder über den Kommandozeilenmodus, Kapitel 15).

## 7 Netzwerke verwalten

Ein Netz besteht aus Name, CIDR (z. B. 192.168.10.0/24) und optional Gateway und Kommentar.

- **Manuell anlegen:** Name und CIDR eingeben; ungültige Angaben werden sofort gemeldet.
- **TXT/CSV importieren:** Datei-Dialog. Format ohne Kopfzeile: Name<Tab>CIDR. Mit Kopfzeile: Subnet Identifier<Tab>Name<Tab>Subnet<Tab>Subnetzmaske. Nach dem Import meldet OTScan die Zahl der neuen Netze.
- **Excel importieren:** erstes Tabellenblatt mit Spaltenüberschriften Subnet Identifier (Netz, z. B. 10.1.2.0/24) und Name, optional Subnetzmask und Gateway. Zeilen ohne gültiges Netz werden übersprungen.

## 8 Scan-Profil und Portsets

Ein **Profil** bündelt die Nmap-Parameter (Scan-Art, Timing, Timeouts, NSE-Skripte). Das **Portset** legt fest, welche Ports geprüft werden. Alle Profile laufen mit dem langsamen Nmap-Timing -T2, Pausen zwischen den Paketen und einer begrenzten Paketrage.

**Nur mit Genehmigung des Netzbetreibers. Für SPS und andere Steuerungen die schonenden Profile verwenden.** Profile mit Betriebssystemerkennung (-O), UDP (-sU) und NSE-Skripten erzeugen deutlich mehr und ungewöhnlichere Pakete. FORCE gehört ausschließlich in Wartungsfenster oder Testumgebungen.

### 8.1 Die Standardprofile

| Profil                                          | Zweck                                                                                                                                                                                                                             | Rechte               | Belastung / Risiko für OT-Geräte                    | Empfohlene Einsatzsituation                                                                                              |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Discovery v2 (saubere Ports, schonend)</b>   | Erste Bestandsaufnahme: TCP-Connect-Scan über wenige, in OT-Netzen typische Ports, leichte Dienst-Erkennung, kein Betriebssystem-Fingerprinting; nur das Nmap-Standardskript <code>knx-gateway-discover</code>                    | keine                | <b>sehr gering</b> (max. 50 Pakete/s, 200 ms Pause) | Erster Durchlauf, Produktivnetze während des Betriebs; Grundlage für den gezielten OT-Tiefenscan                         |
| <b>S7/Legacy schonend (NSE, geräteschonend)</b> | Vollständige Inventur mit SYN-/UDP-Scan, OS-Erkennung, Dienst-Erkennung (Stufe 5) und fokussiertem NSE-Satz (S7, Modbus/Energiemessgeräte, OPC UA, CODESYS, KNX, SNMP, SMB); lange Host-Zeitgrenze (20 min) für träge Steuerungen | Administrator / root | <b>gering</b>                                       | Regelbetrieb nach Abstimmung mit dem Betreiber; auch für empfindliche Alt-SPSen. Richtwert: mehrere Stunden je / 25-Netz |

| Profil                                               | Zweck                                                                                                                                                         | Rechte               | Belastung / Risiko für OT-Geräte                    | Empfohlene Einsatzsituation                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>OT-Tiefenscan CORE (Stufe 2, gezielt)</b>         | Tiefenscan der OT-Ports mit zuverlässigen NSE-Skripten (S7, Energiemessgeräte, OPC UA, BACnet, CODESYS, KNX), Skript-Zeitgrenze 180 s, Host-Zeitgrenze 30 min | Administrator / root | <b>mittel</b> (BACnet-Enumeration und OS-Erkennung) | Nur im Wartungsfenster, bevorzugt gezielt auf die in Stufe 1 erkannten OT-Geräte (Schaltfläche „OT-CORE auf OT-Hosts (letzter Lauf)“) |
| <b>Ohne NSE (Admin)</b>                              | SYN-/UDP-Scan mit Betriebssystem- und Versionserkennung, ohne Geräteabfragen                                                                                  | Administrator / root | <b>mittel</b> (OS-Fingerprinting)                   | Gründliche Port-Inventur, wenn keine Protokollabfragen gewünscht sind                                                                 |
| <b>IT-Sweep (optional, IT-Ports separat)</b>         | Allgemeine IT-Dienste (Datenbanken, Mail, Web, Verzeichnisdienste) mit SMB/HTTP-Skripten                                                                      | Administrator / root | <b>gering bis mittel</b> (bis 100 Pakete/s)         | Ergänzender Rundumblick auf IT-Dienste in OT-Netzen                                                                                   |
| <b>Voll umfassend FORCE (alle Scripts erzwingen)</b> | Erzwingt alle Skripte auf jedem offenen Port (Präfix + ), volle Versions-Erkennung, breites Portset                                                           | Administrator / root | <b>hoch</b>                                         | Nur Wartungsfenster oder Labor: Datensammlung, OT-Dienste auf untypischen Ports. Nicht für den Regelbetrieb                           |

In der Profilliste der Anwendung tragen einige Profilnamen zusätzlich ein Kürzel in eckigen Klammern; gemeint sind dieselben Profile.

#### Empfohlener Ablauf in Produktionsnetzen:

1. „Discovery v2“ über das ganze Netz (kein Administrator nötig, sehr geringe Last).
2. Im Wartungsfenster: Schaltfläche **„OT-CORE auf OT-Hosts (letzter Lauf)“** im Run-Reiter. OTScan übernimmt die im letzten Lauf erkannten OT-Geräte (offene OT-Ports oder OT-Geräteklasse) und scannt nur diese mit „OT-Tiefenscan CORE“ im Hintergrund.
3. Für den Regelbetrieb „S7/Legacy schonend“.

**Hinweis zu FORCE:** Nmap 7.98 und 7.99 können beim Erzwingen von Skripten auf großen, aktiven Netzen abstürzen. OTScan erkennt einen Absturz und wiederholt den Lauf automatisch ohne erzwungene Skripte, notfalls ohne NSE. Bereits fertige Hosts werden aus der Teil-XML gerettet.

## 8.2 Portsets

| Portset      | Umfang          | Verwendung                                                                                            |
|--------------|-----------------|-------------------------------------------------------------------------------------------------------|
| ICS_LIGHT_v2 | 19 TCP + 5 UDP  | Standard von „Discovery v2“: die in OT-Netzen tatsächlich häufig offenen Ports                        |
| ICS_OT_CORE  | 43 TCP + 17 UDP | Standard von „S7/Legacy schonend“, „OT-Tiefenscan CORE“ und „Ohne NSE (Admin)“: bekannte OT/ICS-Ports |
| ICS_IT_SWEEP | 27 TCP + 6 UDP  | Standard von „IT-Sweep“: allgemeine IT-Dienste                                                        |

| Portset      | Umfang                            | Verwendung                                   |
|--------------|-----------------------------------|----------------------------------------------|
| ICS_LIGHT    | 11 TCP + 2 UDP                    | sehr kleine Auswahl der wichtigsten OT-Ports |
| ICS_STANDARD | 101 TCP + 26 UDP                  | breite OT- und IT-Auswahl                    |
| ICS_FULL     | 104 TCP + 29 UDP                  | Standard von FORCE, größte Abdeckung         |
| NONE         | Nmap-Standardports (ca. 1000 TCP) | keine feste Liste                            |

Profile ohne UDP-Scan verwenden automatisch nur den TCP-Teil eines Portsets. Die genauen Portlisten zeigt der Hilfe-Reiter „Portsets“ im Bereich Scan-Typen.

### 8.3 Eigene Profile

Im Bereich **Scan-Typen** können Sie Profile anlegen, duplizieren und ändern. Ändern Sie am besten eine Kopie. „**Profile zurücksetzen**“ stellt die Standardprofile wieder her.

## 9 Scan durchführen (Run)

1. **Netzwerk** wählen.
2. **Profil** und **Portset** wählen (das Portset folgt dem Profil-Standard und kann geändert werden).
3. Optional unter „Erweiterte Optionen“ die **Netzwerkschnittstelle** wählen (bei mehreren Adaptern).
4. **Ausgabe-Ordner** festlegen.
5. **Export-Auswahl**: XML entsteht immer (Nmap-Rohdaten); **Excel**, **PDF** und **PowerPoint** sind einzeln an- oder abwählbar.
6. „**Job hinzufügen**“ – so lassen sich mehrere Netze in eine Warteschlange stellen; bis zu 6 Jobs laufen parallel.
7. „**Queue starten**“, im Bestätigungsfenster die drei Punkte bestätigen.

Während des Scans zeigen Fortschrittsbalken, Statusspalte und Protokoll den Stand. „Stop selektiert“ und „Stop alle“ beenden laufende Scans. Nach dem Scan meldet OTScan Veränderungen gegenüber dem letzten Scan desselben Netzes und bietet an, die Reports zu öffnen.

**Reports neu erzeugen**: „XML → Excel/PDF“ baut Reports aus einer vorhandenen Nmap-XML, „Reports für selektierten Job neu erzeugen“ aus der Warteschlange – jeweils gemäß aktueller Export-Auswahl.

## 10 NSE-Skripte

OTScan liefert **22 NSE-Skripte** (davon 20 OT-spezifisch) und **2 Lua-Bibliotheken** mit. Sie sind in der Programmdatei eingebettet und werden automatisch verwendet – ein Kopieren in den Nmap-Ordner ist nicht mehr nötig. Zusätzlich nutzen die Profile Standardskripte, die in jeder Nmap-Installation enthalten sind (z. B. `banner`, `snmp-info`, `http-title`, `modbus-discover`, `enip-info`, `knx-gateway-info`).

- Ist ein Skript in der installierten Nmap vorhanden, wird es über den Namen aufgerufen, sonst aus OTScan.
- Fehlt ein Skript in beiden, lässt OTScan es vor dem Start weg und vermerkt das im Protokoll, statt den Scan abzurechnen.
- Eigene oder aktualisierte Skripte legen Sie unter `%APPDATA%\OTScan\nse_scripts` (Linux: `~/local/share/OTScan/nse_scripts`) ab; sie haben Vorrang.

Liste, Zweck und Einsatz aller Skripte beschreibt die separate **NSE-Skripte-Dokumentation**.

## 11 Risiko-Ampel

Die Ampel bewertet offene Ports anhand einer Liste von **51 bewerteten Port-Einträgen: 27 OT-Einträge** (18 OT-/ICS-Protokolle, teils mit TCP- und UDP-Variante) und **24 unsichere IT-Protokoll-Einträge**. Jeder Eintrag hat ein Gewicht von 1 bis 3.

**Die Ampel ist keine Konformitätsbewertung nach IEC 62443** (und auch nicht nach BSI, NIST oder CISA). Die Zuordnung Port → Protokoll folgt öffentlichen Registern (IANA, Herstellerspezifikationen). Die **Gewichte und Schwellen sind eine interne Heuristik** von OTScan, keine Normvorgabe. Die Ampel ist ein Hinweis zur Priorisierung, keine abschließende Risikoanalyse.

### 11.1 Gewichtung

| Gewicht | Bedeutung                                                                                                                 | Beispiele                                                                                                                                                                                                                                                                                                                                           |
|---------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3       | OT-Protokoll erlaubt in der Regel unauthentifiziertes Lesen, Schreiben oder Stoppen; IT-Dienst gilt als „nicht verwenden“ | S7comm (102/tcp), Modbus/TCP (502/tcp), DNP3 (20000/tcp), EtherNet/IP (44818/tcp), IEC 60870-5-104 (2404/tcp), Omron FINS (9600/udp), PC WORX (1962/tcp), ProConOS (20547/tcp), CODESYS V2 (2455/tcp), GE SRTP (18245/tcp), MELSEC-Q (5007/tcp); Telnet, SMB, VNC, rexec/rlogin/rsh                                                                 |
| 2       | Discovery-, Gebäude- oder Zweittransport ohne Authentisierung; IT-Klartextprotokoll                                       | Modbus/UDP, DNP3/UDP, EtherNet/IP UDP und I/O (2222/udp), BACnet/IP (47808/udp), PROFINET CM (34964/udp), Niagara Fox (1911/tcp), Omron FINS/TCP, HART-IP (5094/tcp), CODESYS Gateway (1200/tcp) und V3 (11740/tcp), MELSEC-Q/UDP (5006/udp), Red Lion Crimson (789/tcp), KNXnet/IP (3671/udp); FTP, HTTP, 8080, VNC-HTTP, RPC, NetBIOS, SNMP v1/v2 |
| 1       | Protokoll mit optionaler Sicherheit – Einstellungen prüfen; IT-Klartext mit geringerer Tragweite                          | OPC UA (4840/tcp), HART-IP/UDP; SMTP, POP3, IMAP, LDAP, LDAP-GC, Portmapper, NFS, rwho                                                                                                                                                                                                                                                              |

### 11.2 Ampelregeln

Pro Gerät werden die Gewichte aller offenen bewerteten Ports addiert (Gesamtwert) und der OT-Anteil getrennt geführt.

| Stufe | Regel pro Gerät                                               | Beispiel                                                     |
|-------|---------------------------------------------------------------|--------------------------------------------------------------|
| ROT   | Gesamtwert $\geq 6$ und OT-Anteil $\geq 3$                    | S7 + Modbus (6, OT 6); Telnet + Modbus (6, OT 3)             |
| GELB  | mindestens ein bewerteter Port offen, ROT-Regel nicht erfüllt | nur S7 (3); Modbus + OPC UA (4); Telnet + SMB (6, aber OT 0) |
| GRÜN  | kein bewerteter Port offen                                    | nur SSH und HTTPS                                            |
| INFO  | Gerät erreichbar, lieferte aber keine Portdaten               | verstummtes oder sehr langsames Gerät                        |

Das Netz (der Scan) erhält **ROT**, sobald ein Gerät ROT ist, sonst **GELB**, wenn irgendwo ein bewerteter Port offen ist, sonst **GRÜN**; liegen nur Geräte ohne Portdaten vor, **INFO**. Die vollständige Portliste steht im PDF-Anhang und in docs\OTScan\_RiskScoring\_Quellen\_Methodik.txt.

## 12 Berichte

---

Reports entstehen im gewählten Ausgabe-Ordner mit dem Namen <Netz>\_<Zeitstempel> (.xml, .xlsx, .pdf, .pptx) sowie einer Protokolldatei.

**Excel:** Blätter *Summary* (Kennzahlen, Ampel), *Hosts* (IP, MAC, Hersteller, Geräteklasse, offene Ports, bewertete Ports, OT- und IT-Anteil, OS, Hostnamen, S7-/BACnet-Details), *Ports*, *Scripts* (NSE-Ausgaben), *Delta* (Änderungen zum letzten Scan) und – falls hinterlegt – *Firewall\_Flows* / *Firewall\_Top\_Flows*; bei konfiguriertem Inventar zusätzlich *CMDB Ansicht* und *Shadow* (nicht in CMDB).

**PDF:** Deckblatt mit Scan-Informationen, Executive Summary mit Kennzahlen, Trend zum letzten Scan, Key Findings und Handlungsempfehlungen, Netzwerk-Heatmap und Gerätetyp-Verteilung, Detailansicht kritischer Hosts, Host-Inventar, Delta-Report, technischer Anhang (bewertete Ports, Nmap-Argumente, ggf. Firewall-Kommunikation), ICS/OT-Glossar sowie „Quellen & Verankerung der Risikobewertung“. Bei 0 gefundenen Geräten entsteht ein einseitiger Bericht „Keine aktiven Geräte gefunden“.

**PowerPoint:** kompakte Management-Zusammenfassung je Scan (Kennzahlen, Top-Ports, auffällige Geräte, Trend). Optional wird ein Manager-Sammeldeck über mehrere Scans fortgeschrieben.

Ein **Muster-Report** mit fiktiven Daten liegt im Ordner *Muster-Report* bei.

## 13 Weitere Funktionen

---

### 13.1 History und Delta

Die History listet alle Scans mit Zeitpunkt, Netz, Profil und Ergebnis. Zwei Scans desselben Netzes lassen sich vergleichen: neue und verschwundene Geräte, geänderte Ports, geänderte bewertete Ports, Hersteller- und OS-Änderungen. Der Vergleich kann als Excel gespeichert werden.

### 13.2 Inventar-Abgleich (CMDB)

Vergleicht die Scan-Ergebnisse mit einem Soll-Inventar aus Excel. Erwartet wird ein Tabellenblatt „**CMDB**“ mit Daten ab Zeile 18; maßgeblich sind die IP-Adresse (Spalte AB) und die MAC-Adresse (Spalte AF), weitere Spalten (Name, Hersteller, Betriebssystem, Standort, Subnetz) werden angezeigt. Ergebnis je Gerät: *OK*, *MAC geändert*, *IP geändert*, *Offline – nicht im Scan gefunden*, *Neu – nicht in CMDB*. Der Abgleich kann als Excel-Bericht exportiert oder – auf ausdrücklichen Wunsch – in die CMDB-Datei zurückgeschrieben werden (vorher Sicherung anlegen).

### 13.3 Hersteller/OS-Regeln

Nmap leitet Hersteller aus der MAC-Adresse ab; das ist bei OEM-Geräten oft ungenau. Unter **Hersteller/OS** legen Sie Regeln an (nach Herstellertext, MAC-Präfix oder IP), die Hersteller und Betriebssystem in allen neuen Reports überschreiben. Regeln lassen sich exportieren, importieren und aus der CMDB ableiten.

## 13.4 Splunk-DB (Firewall-Kommunikation)

Über **Splunk-DB** hinterlegen Sie je Netz einen Splunk-XML-Export der Firewall-Kommunikation (Felder u. a. `source`, `destination`, `protocol`, `ports`, `count`). Bei jedem Scan des Netzes werden die Flows automatisch in Excel und PDF eingearbeitet (beobachtete Verbindungen, kritische und geblockte Flows).

## 14 Branding: eigenes Logo im Report

Legen Sie im Datenordner eine Datei `branding_config.json` an:

```
{"logo_report": "mein_logo.png", "company_name": "Muster GmbH"}
```

und kopieren Sie `mein_logo.png` in denselben Ordner (Windows: `%APPDATA%\OTScan`, Linux: `~/.local/share/OTScan`). Relative Dateinamen gelten relativ zu diesem Ordner. `logo_report` erscheint im PDF-Report und in der Seitenleiste, `company_name` als Name in der Seitenleiste. Weitere Schlüssel: `icon` (Fenstersymbol, `.ico`) und `logo_small` (32-px-Logo). Fehlt die Datei oder ist sie fehlerhaft, verwendet OTScan das Standard-Branding. Alternativ wird die Datei auch neben der Programmdatei gesucht (portable Nutzung).

## 15 Kommandozeilen- und Headless-Modus

OTScan kann den gezielten OT-Tiefenscan ohne Oberfläche ausführen:

```
OTScan_v2.0.1.exe --ot-core-targeted "<Netzname>"      (Windows)
./OTScan --ot-core-targeted "<Netzname>"              (Linux, für Tiefenscans mit sudo)
```

OTScan nimmt den jüngsten erfolgreichen Lauf dieses Netzes aus der Datenbank, ermittelt die OT-Geräte und scannt nur diese mit dem Profil „OT-Tiefenscan CORE“ und dem Portset `ICS_OT_CORE`. Excel und PDF entstehen im Ordner des vorherigen Laufs. Das Protokoll steht in `scheduler.log` im Datenordner (die Windows-Programmdatei öffnet kein Konsolenfenster).

| Rückgabewert | Bedeutung                                                               |
|--------------|-------------------------------------------------------------------------|
| 0            | fertig (oder keine OT-Geräte im vorherigen Lauf)                        |
| 1            | Nmap meldete einen Fehler                                               |
| 2            | Aufruf fehlerhaft, kein vorheriger Lauf, XML oder Profil nicht gefunden |
| 4            | keine gültige Lizenz und Testphase abgelaufen                           |

Voraussetzung ist ein vorheriger Lauf (z. B. „Discovery v2“) aus der Oberfläche. Der Kommandozeilenmodus unterliegt derselben Lizenzprüfung wie die Oberfläche. Geplante Scans (`--scheduled-scan`) sind in 2.0.1 deaktiviert und enden mit Rückgabewert 3.

## 16 Fehlerbehebung

| Symptom                                                                                                         | Ursache / Lösung                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scan startet nicht, im Protokoll „nmap“ nicht gefunden                                                          | Nmap ist nicht installiert oder nicht im <code>PATH</code> . Nmap von <a href="http://nmap.org">nmap.org</a> installieren; in einer neuen Eingabeaufforderung <code>nmap --version</code> prüfen; ggf. <code>C:\Program Files (x86)\Nmap</code> zum <code>PATH</code> hinzufügen und OTScan neu starten.<br>Linux: <code>sudo apt install nmap</code>       |
| SYN-/UDP-/OS-Scan schlägt fehl, Meldungen zu Npcap, „dnet“ oder „Only ethernet devices...“, oder Nmap stürzt ab | <b>Npcap fehlt oder ist defekt.</b> Npcap (über den Nmap-Installer oder <a href="http://npcap.com">npcap.com</a> ) mit Administratorrechten neu installieren und den Rechner neu starten. Solange Npcap fehlt, nur „Discovery v2“ verwenden                                                                                                                 |
| Bestätigungsfenster zeigt „Keine Administrator-Rechte – Profil erfordert Admin“                                 | OTScan über die Neustart-Option im Fenster oder per Rechtsklick „Als Administrator ausführen“ starten. Linux: <code>sudo ./OTScan</code>                                                                                                                                                                                                                    |
| Profil bricht ab oder liefert keine NSE-Ergebnisse; Protokoll meldet ausgelassene Skripte                       | Nicht vorhandene Skripte werden vor dem Start <b>ausgelassen</b> (Warnung im Protokoll). Lädt Nmap die Skripte nicht (NSE-Initialisierungsfehler), wiederholt OTScan den Scan einmal <b>ohne NSE</b> , damit ein Report entsteht. Nmap auf eine aktuelle Version bringen; eigene Skripte in <code>nse_scripts</code> im Datenordner auf Syntaxfehler prüfen |
| FORCE stürzt ab (Exit 0xC0000409 oder 0xC06D007E)                                                               | Bekanntes Nmap-7.98/7.99-Problem bzw. Npcap-Fehler. OTScan wiederholt automatisch ohne erzwungene Skripte. Für den Regelbetrieb „S7/Legacy schonend“ nutzen                                                                                                                                                                                                 |
| Wenige Ports auf SPSen gefunden                                                                                 | Träge Steuerungen brauchen länger. „S7/Legacy schonend“ (Host-Zeitgrenze 20 min) verwenden                                                                                                                                                                                                                                                                  |
| Linux: nach <code>sudo ./OTScan</code> erscheint kein Fenster                                                   | Wayland: <code>xhost +SI:localuser:root</code> ausführen, dann erneut starten                                                                                                                                                                                                                                                                               |
| Linux: Programm startet nicht, Meldung zu <code>GLIBC_2.xx</code>                                               | Distribution zu alt ( <code>glibc &lt; 2.31</code> ). Neuere Distribution verwenden                                                                                                                                                                                                                                                                         |
| Nach Start als Administrator erscheint wieder der Aktivierungsdialog                                            | Anderes Benutzerkonto (eigenes Profil). Schlüssel dort einmal über „Lizenz eingeben...“ eingeben                                                                                                                                                                                                                                                            |
| „Die Lizenzprüfung konnte nicht ausgeführt werden“                                                              | Details in <code>license_error.log</code> im Datenordner; OTScan neu installieren bzw. Support kontaktieren                                                                                                                                                                                                                                                 |
| Kein PDF/Excel nach dem Scan                                                                                    | Export-Auswahl im Run-Reiter prüfen; Report mit „XML → Excel/PDF“ neu erzeugen; ist eine gleichnamige Excel-Datei geöffnet, schreibt OTScan unter einem neuen Namen                                                                                                                                                                                         |

## 17 Rechtliches und Datenschutz

**Nmap und NSE-Skripte:** Nmap ist nicht Bestandteil von OTScan und steht unter der Nmap Public Source License (NPSL). Alle mitgelieferten NSE-Skripte und -Bibliotheken – auch die eigenen – stehen unter „Same as Nmap“ (NPSL) und sind nicht Teil der kostenpflichtigen OTScan-Lizenz. Details: `THIRD_PARTY_NOTICES.txt` und `LICENSE_NPSL_Nmap.txt` im Paket.

**OTScan-Lizenz:** Es gilt die `EULA.txt`; die Nutzungs- und Haftungshinweise in `HAFTUNG_UND_NUTZUNG.txt` sind Bestandteil der EULA.

**Datenschutz:** Scan-Ergebnisse, Netzbereiche und Reports bleiben auf Ihrem Rechner. Einzige Datenübertragung ist die Lizenzaktivierung (Abschnitt 5.3): Lizenzschlüssel (mit Name und Bestellnummer), gehashte Geräte-ID und technisch bedingt die IP-Adresse an den Lizenzserver (Cloudflare, USA). Kein Tracking, keine Telemetrie. Weitere Informationen in der Datenschutzerklärung auf [hanselcraft.de](https://hanselcraft.de).

**Herausgeber:** Jörg Hansel, HanselCraft · [hanselcraft.de](https://hanselcraft.de)