TECHNIK · SICHERHEIT · DATENSCHUTZ

Technik, Sicherheit und Datenschutz

Verbindungen, Netzwerkverkehr, Bewertungslogik, Datenhaltung, Importe, Schutzmaßnahmen, Drittkomponenten und KI-Assistent.

Version 3.0.0 · Stand 12.11.2026
HanselCraft · otscan.hanselcraft.de

1 Zweck und Grundsätze

Dieses Dokument beschreibt für IT-Sicherheit, Datenschutz und Betrieb, was OTScan 3 technisch tut, welche Daten entstehen, wo sie liegen und welche Verbindungen das Programm aufbaut. Grundlage ist der Programmstand 3.0.0.

- **Lokal:** Alle Scan-, Inventar- und Berichtsdaten bleiben auf dem Rechner bzw. in Ordnern, die der Anwender wählt.
- **Keine Telemetrie:** OTScan 3 sendet keine Nutzungs-, Absturz- oder Gerätedaten an HanselCraft oder Dritte.
- **Nur lesend:** keine Schreibbefehle an Geräte, keine Passwortversuche, keine nmap-Skripte der Kategorien vuln, brute, exploit oder dos.

2 Verbindungen ins Internet

Funktion	Wann	Ziel	Was wird übertragen
Lizenz aktivieren	beim Klick auf **Aktivieren**; war der Server dabei nicht erreichbar, holt OTScan 3 die Aktivierung beim Programmstart nach (höchstens einmal je 24 Stunden), bis sie gelungen ist	Lizenzserver von HanselCraft (HTTPS)	Lizenzschlüssel, Rechnerkennung (SHA-256-Prüfwert aus Rechnername und MAC-Adresse, gekürzt – nicht umkehrbar), Programmversion, Produktkennung
Rechner freigeben	nur beim Klick auf „Diesen Rechner freigeben“	Lizenzserver (HTTPS)	Lizenzschlüssel und Rechnerkennung
Herstellermeldungen aktualisieren	nur beim Klick auf **Online aktualisieren**	öffentliche CSAF-Quellen (z. B. Siemens ProductCERT, CERT@VDE, BSI, Bosch PSIRT, CISA), CISA-KEV-Liste, FIRST-EPSS	nur Abrufe öffentlicher Dateien – keine Daten über Ihre Geräte oder Netzwerke
KI-Assistent (optional)	nur, wenn Sie einen Assistenten (z. B. Claude Desktop) einrichten und ihm Fragen stellen	Anbieter des Assistenten (z. B. Anthropic) – die Verbindung baut der Assistent auf, nicht OTScan 3	was der Assistent über die Schnittstelle liest: Netznamen, IP- und MAC-Adressen, Gerätenamen, Hersteller, offene Ports, Befunde, Fristen (siehe Abschnitt 10)

Ohne Internet funktioniert OTScan 3 vollständig: Die Lizenzprüfung im Betrieb läuft offline mit einer signierten Lizenzdatei (öffentlicher Schlüssel im Programm). Die Herstellermeldungen lassen sich auch auf einem anderen PC mit `otsp_csaf_sync.py` erzeugen und mit „Datei übernehmen …“ einspielen.

Proxy: Für diese Abrufe nutzt OTScan 3 die Proxy-Einstellungen des Systems (Umgebungsvariablen HTTPS_PROXY/HTTP_PROXY, unter Windows auch die Systemeinstellung). Mail-Entwürfe der Erstinbetriebnahme werden nur als Datei (Outlook-Entwurf bzw. `.eml`) angelegt und nie gesendet.

3 Netzwerkverkehr im Anlagennetzwerk

Stufe	Verkehr
0 Nachbar-Erkennung	ARP-Anfragen (höchstens 20 Pakete/s); ohne Administratorrechte ein kurzer TCP-Verbindungsversuch je Adresse
1 Geräte finden	TCP-Verbindungsaufbau auf feste OT-Portlisten (höchstens 50 Pakete/s), nur belegte Adressen
2a Dienste	Versionsproben an offene Ports, nur lesende OT-Abfragen (z. B. S7-Identität, Modbus-Geräte-ID nur auf Wunsch)
2b Namen	wenige UDP-Standardabfragen (SNMP GET mit „public“, BACnet, KNX)
CAM	WS-Discovery und ONVIF GetDeviceInformation (nur lesend); mit hinterlegtem Zugang höchstens 3 Fehlanmeldungen je Lauf

Ein Netzwerk, ein Scanner: OTScan 3 warnt vor fremden nmap-Prozessen. Der Freigabe-Haken („Freigabe des Anlagenverantwortlichen liegt vor“) gilt 30 Tage und ersetzt keine schriftliche Freigabe. Zeitplan und Netzwerkkette laufen unbeaufsichtigt – nur mit organisatorischer Freigabe.

4 Bewertungslogik

Unsichere Dienste werden nach den **Verkehrsregeln** bewertet – einer HanselCraft-Voreinstellung, angelehnt an IEC 62443 (Zonen und Conduits) und allgemeine OT-Sicherheitspraxis. Sie ist keine Norm und kein Normzitat. Gewicht 3: Dienste mit Fernsteuerung, Befehlsausführung oder Dateizugriff (Telnet, R-Kommandos, VNC, FTP, SMB); 2: Klartext-Anmeldung oder Informationsabfluss (HTTP, SNMPv1/v2c, NetBIOS, RPC, NFS, LDAP …); 1: Zweittransporte oder Dienste, die verschlüsselt zulässig sein können. Ein offener Port aus der Liste ergibt GELB. Anpassung: `verkehrsregeln.json` im Datenordner.

Herstellermeldungen: Erkannte Modelle und Firmwarestände werden offline mit dem mitgelieferten CSAF-Bestand abgeglichen (Güte exakt, modell, hersteller), ergänzt um CISA KEV und EPSS.

5 Datenhaltung

Daten	Windows	Linux
Datenbank, Einstellungen, Scan-MAC-Liste, Zeitpläne, Hersteller-Regeln, Verkehrsregeln, Dokumentations-Datenbank	`%APPDATA%\OTScan3`	`~/.local/share/OTScan3`
Scan-Ergebnisse (XML) und Berichte	Ausgabeordner (Standard: Dokumente)	Dokumente-Ordner
Inventar, Splunk-Ablage, Abnahmen, Vorlagen, Sicherungen	Dokumente\OTScan3_...	Dokumente/OTScan3_...
Kamera-Passwörter	verschlüsselt mit Windows DPAPI (an das Benutzerkonto gebunden)	Schlüsselbund (secret-tool)
Lizenz	signierte Lizenzdatei im Datenordner	ebenso
KI-Assistent: Einstellung, Freigabecode (nur als HMAC), Protokoll	`%APPDATA%\OTScan3\ki_assistent.json`, `ki_schnittstelle.log`	`~/.local/share/OTScan3/…`
KI-Assistent: geheimer Schlüssel je Installation	`%LOCALAPPDATA%\HanselCraft\OTScan3\ki.schluessel`, mit DPAPI an das Benutzerkonto gebunden	`~/.config/hanselcraft-otscan3/ki.schluessel` (nur gültig mit Rechten 0600 und als Datei des Benutzers)
KI-Assistent: Stand-Zähler	`ki.stand` neben dem Schlüssel (unterschrieben)	`ki.stand` neben dem Schlüssel (unterschrieben)

Die Datenbank ist nicht verschlüsselt. Schutz über das Benutzerprofil und die Laufwerksverschlüsselung des Rechners. Alle Ausgaben enthalten IP-Adressen, MAC-Adressen, Gerätenamen und Standorte und sind vertraulich zu behandeln. Personenbezogene Daten entstehen nur, wenn Anwender sie selbst eintragen (z. B. Name und Telefon des Technikers in der Erstinbetriebnahme oder Verantwortliche in der CMDB).

6 Datenimporte

- **Inventar (CMDB):** Excel-Datei, wird nur gelesen; Nachträge entstehen als Kopie.
- **Firewall-Logs:** generischer Import von Exporten (z. B. Splunk-Suche über FortiGate-Logs, Format v2: `<Netzwerk>_<von>_<bis>_regeln.csv` und `_inventar.csv`); keine Verbindung zu Splunk selbst.
- **Dokumentation:** JSON-Import für Applikationen, Systeme und Netzwerkbereiche.

7 Schutz bei Administratorrechten

Unter Windows liegt das Programm in `C:\Program Files\OTScan3` (nur Administratoren können es ändern). Mit Administratorrechten startet OTScan 3 nmap nur aus geschützten Ordnern und nur mit Optionen aus einer festen Liste; Skripte nur aus dem nmap-Programmordner. Unter Linux erhält nmap nur für die Gruppe `otscan3` die Capability `cap_net_raw`; Adapter stellt ein Helfer mit fest geprüften Argumenten und nur für freigegebene Adapter um.

8 Aufbewahrung und Löschen

OTScan 3 löscht nichts automatisch. Aufbewahrungsfristen legt der Betreiber fest. Ein Netzwerk vollständig löschen: Programm beenden, Dateien mit dem Netzwerknamen im Ausgabeordner und in den Unterordnern OTScan3_Inventar und OTScan3_Splunk entfernen, Zustandsdateien unter `…\OTScan3\stufenlauf` löschen und das Netzwerk in der Datenpflege entfernen. Datensicherungen (ZIP) enthalten dieselben Daten.

9 Drittkomponenten

nmap (Nmap Public Source License, separat installiert), Npcap (eigene Lizenz, Windows), Python und Bibliotheken (openpyxl, python-pptx, Pillow, fpdf2, lxml, pandas), Schriften Inter und Bricolage Grotesque (SIL OFL), Symbole Lucide (ISC). Die Lizenztexte liegen im Programmordner (`THIRD_PARTY_NOTICES.txt`, `LICENSE_NPSL_Nmap.txt`, `assets/LIZENZ_*`). Nutzungsbedingungen: `EULA.txt` und `HAFTUNG_UND_NUTZUNG.txt`.

10 KI-Assistent (optional)

Über die Seite **KI-Assistent** lässt sich OTScan 3 als lokale MCP-Schnittstelle (Model Context Protocol) in einen Assistenten wie Claude Desktop eintragen. Die Schnittstelle ist eine **lokale Brücke**: Der Assistent startet sie als Programm auf demselben Rechner und spricht über Standardein- und -ausgabe mit ihr. Sie öffnet keinen Netzwerkanschluss und baut selbst keine Internetverbindung auf.

- **Lesen:** nur die Datenbank von OTScan 3, nur lesend (Netze, Scan-Läufe, Geräte, Befunde, Nachweise & Fristen).
- **Übertragung:** Was der Assistent liest, schickt er zur Verarbeitung an seinen Anbieter (z. B. Anthropic). Dazu gehören IP- und MAC-Adressen, Geräte- und Netznamen, Hersteller, offene Ports und Befunde.

Klären Sie vorher, ob diese Daten Ihr Haus verlassen dürfen, und beachten Sie die Bedingungen des Anbieters. Ohne Eintrag im Assistenten ist die Schnittstelle nicht aktiv.

- **Scans durch die KI:** standardmäßig aus. Erst mit dem Haken „KI darf Scans starten“ und einem sechsstelligen Freigabecode, den nur die Oberfläche zeigt (30 Minuten gültig, einmal verwendbar, verfällt nach drei Fehleingaben). Nur angelegte Netze (Name und CIDR), nur private IPv4-Bereiche bis /16, höchstens ein KI-Scan gleichzeitig; ohne gültige Lizenz oder Testphase keine Werkzeuge.
- **Schutz des Codes:** Gespeichert wird nur ein HMAC mit einem geheimen Schlüssel je Installation, der außerhalb des Datenordners liegt (Windows: nur mit DPAPI verschlüsselt – eine unverschlüsselte Schlüsseldatei wird dort nicht angenommen; Linux: nur mit Rechten 0600 als Datei des Benutzers). Schalter und Code sind zusätzlich mit einem fortlaufenden Stand-Zähler unterschrieben: Jede Änderung macht ältere Fassungen der Einstellungsdatei ungültig, verbrauchte und verfallene Codes bleiben auch nach einem Neustart verbraucht. Wer nur die Einstellungsdatei liest oder selbst beschreibt, erhält keinen gültigen Code.

Grenzen: Der Freigabecode schützt vor Scans, die ein Assistent nur über die Schnittstelle anstößt. Wer Schreibzugriff auf das Benutzerprofil hat, kann Schlüssel-, Stand- und Einstellungsdatei gemeinsam auf einen alten Stand zurücksetzen und so einen schon genannten Code wieder gültig machen. Wer Programme unter dem Benutzerkonto ausführen kann (unter Linux: wer den Heimordner lesen oder ändern kann), kann die Freigabe ganz umgehen. Geben Sie dem Assistenten deshalb keine Werkzeuge, die Dateien im Benutzerprofil lesen oder ändern oder Programme ausführen dürfen – auch nicht, solange Scans durch die KI ausgeschaltet sind.