SerNet

// DENIC Spark

Open Source: Lizenz, Copyright, Lieferkette

10. November 2026

Dr. Johannes Loxen

SerNet GmbH, Göttingen – Berlin – San Francisco

SerNet

Über SerNet

1997 gegründet

5000+ Bestandskunden in Deutschland, Europa, USA und weltweit

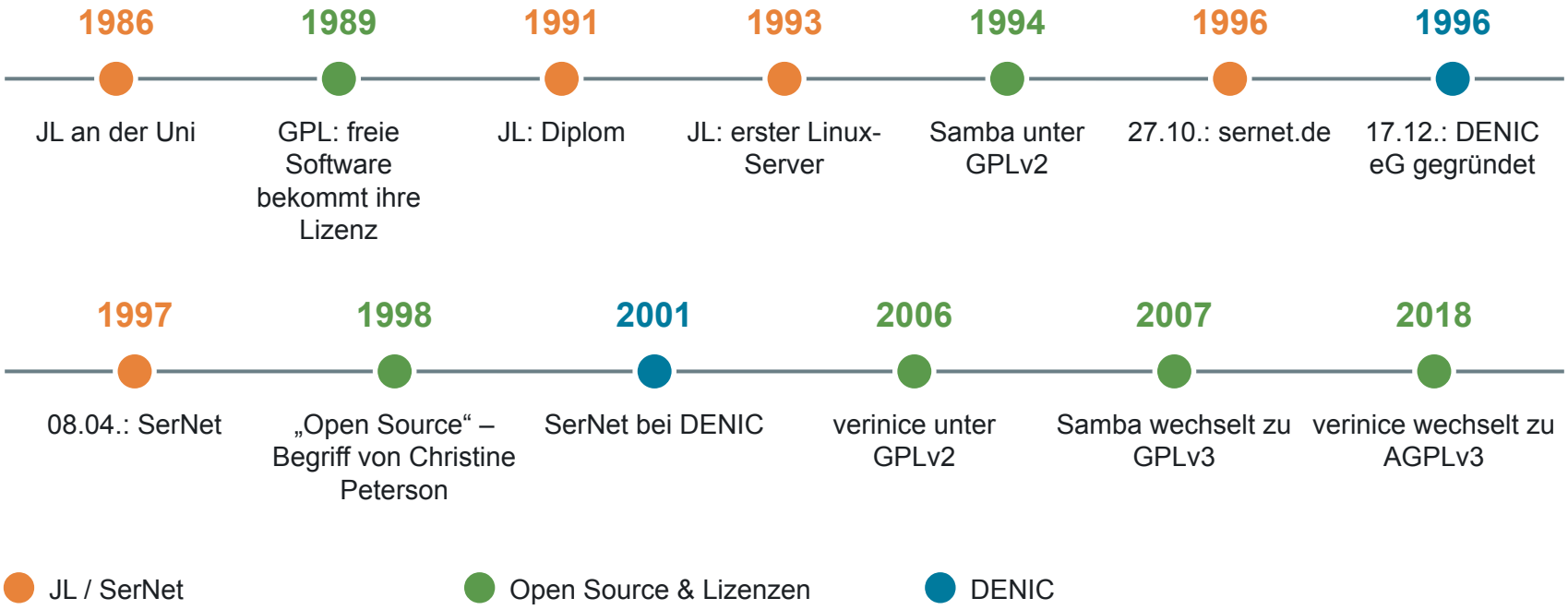
3 Standorte: Göttingen · Berlin · San Francisco (SerNet, Inc.)

- Schwerpunkt Informationssicherheit und Datenschutz
- Sichere IT-Infrastruktur: Firewalls, E-Mail, Archivierung, Virtualisierung, hybride Cloud, Microsoft 365
- Technische Sicherheitslösungen für Industrie und öffentliche Hand
- verinice: Open-Source-Tool für Informationssicherheits-Management
- Samba: Open-Source-Alternative zu Windows-Servern
- Klassischer Mittelstand: in privater Hand, kein Risikokapital, keine Bankkredite

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Von der GPL bis zur AGPL – eine kleine Historie



SerNet

1

// Teil 1

Open Source einsetzen

Fragen aus Sicht der Anwender im Unternehmen

SerNet

Open Source einfach so einsetzen?

Was regelt das Unternehmen?

- Gibt es eine Vorgabe, die Open Source verbietet?
- Darf ich kostenfreie OSS einsetzen – eine Schenkung ohne Garantie?
- Nur offizielle OSI-Lizenzen, keine bloß kostenlose Software?
- Muss Support mit eingekauft werden, zumindest als Option?

Was gilt am Arbeitsplatz?

- Darf ich Software aus dem Internet ohne Genehmigung laden und nutzen?
- Darf ich sie auf dem Firmenrechner einfach installieren?
- Kann ich das als normaler User überhaupt?

SerNet

Lieferkettenrisiken einschätzen

Alles Leitungsentscheidung: Welches Risiko das Unternehmen trägt, legt die Leitung fest.

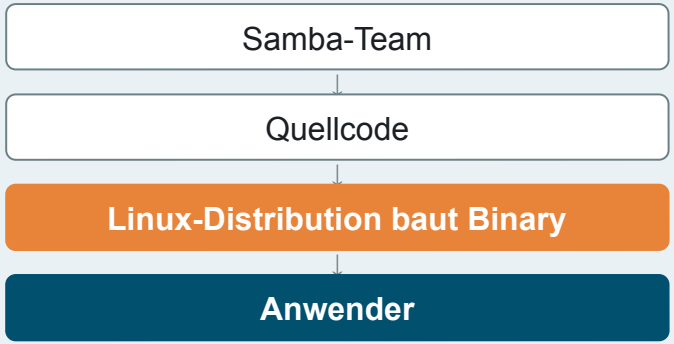
Herkunft
Gibt es beim Lieferanten eine Qualitätssicherung?

Eigene Prüfung
Kann ich die Qualität selbst einschätzen?

Haftung
Bei OSS gilt immer der Haftungsausschluss im Quellcode.

Es gibt auch Open-Source-Trojaner :-)

Kommt das Binary vom Programmierer?



SerNet

NIS2 und CRA aus Anwendersicht

CRA

Pflicht für Anbieter

- Hersteller müssen Konformität nachweisen
- Als Anwender schätze ich das CE-Zeichen, habe aber keine direkten Pflichten
- Wer OSS in eigene Produkte einbaut, wird selbst Hersteller

NIS2

lizenz-agnostisch

- Gilt für jede Software, offen oder proprietär
- Für jede Software den Notfall vordenken

Vorteil Open Source: unter Umständen leichter zu prüfen und bei Problemen leichter durch Alternativen zu ersetzen.

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Muss ich die CE-Kennzeichnung prüfen?



Was steckt hinter dem Zeichen?

- **Nur, wenn das Unternehmen es vorgibt**
  im Rahmen der eigenen Qualitätssicherung
- **Prüfen kann man kaum etwas**
  Bei normaler Software ist der Konformitätsprozess kaum nachvollziehbar – wie beim CE-Logo auf einem Steckernetzteil
- **Modul A heißt Selbsterklärung**
  Für die meisten Produkte bewertet der Hersteller die Konformität selbst

SerNet

2

// Teil 2

Open Source entwickeln

Lizenz, Copyright und die eigene Lieferkette

// Lizenzwahl

Die Lizenzwahl ist die freie Wahl der EntwickelInden.

… und eine Anfangswert-Entscheidung: später kaum mehr zu ändern.

SerNet

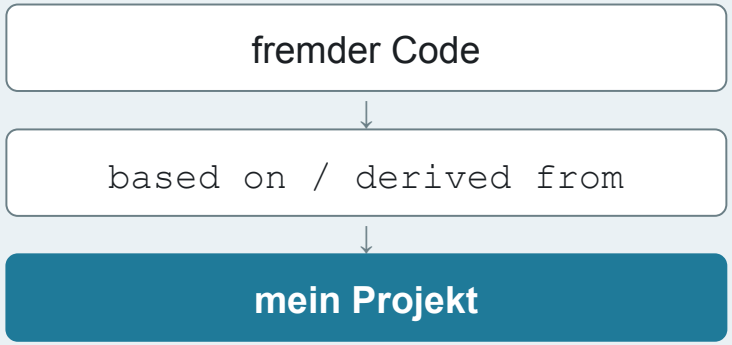
Sorgfalt von Anfang an

Ordentlich(!) lizenzieren

- ✓ Header
- ✓ Autoren
- ✓ Lizenz
- ✓ Haftungsfreistellung

Abhängigkeiten erkennen

aka „Supply Chain“



SerNet

Wem gehört das Copyright?



Persönlich

„echte freie Software“

- Copyright bleibt bei der Person – egal, wo sie arbeitet
- Forschungsfreiheit, wenig Patentprobleme
- Umlizenzierung kaum möglich



Corporate

„unechte freie Software“

- Gewerbliche Software – Patente!
- Umlizenzierbar, dual lizenzierbar
- Haftungsfreistellung im Code kann problematisch werden



Assignment

juristisch sauber, aber „igitt“

- In der Regel per Vertrag
- Arbeitgeber darf die Lizenz ohne Einverständnis der Entwickelnden ändern

SerNet

Jede Lizenzänderung gilt erst ab Stichtag

Bestand bis zum Stichtag
bleibt unter der alten Lizenz – für immer

Neuer Code ab dem Stichtag
steht unter der neuen Lizenz



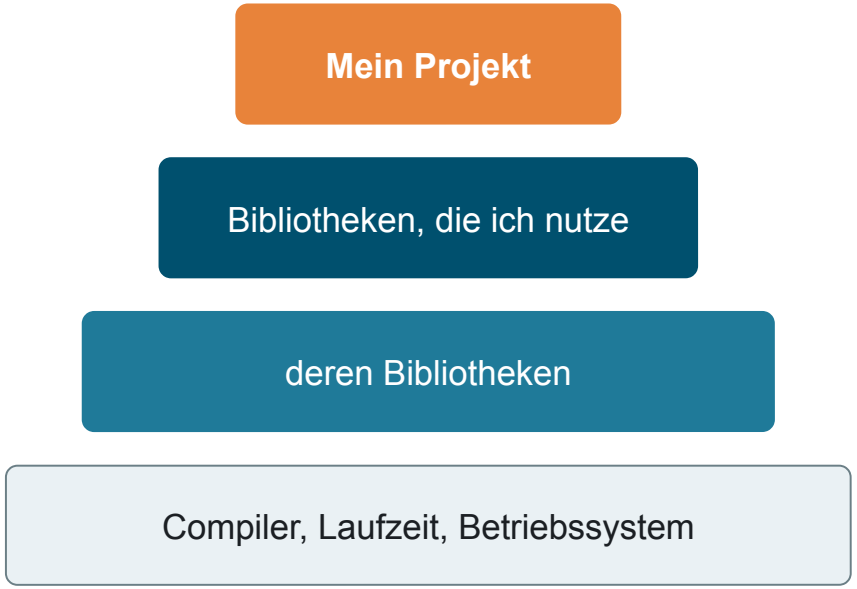
Samba: GPLv2 → GPLv3 (2007)

verinice: GPLv2 → AGPLv3 (2018)

Alte Stände bleiben nutzbar – wenn man den Code noch hat oder mitnehmen darf.

SerNet

Auf wessen Schultern stehe ich?



Welche Bibliotheken nutze ich?
direkt und indirekt – bis in die Tiefe des Abhängigkeitsbaums

Kenne ich die SBOM meiner Lieferanten?
maschinenlesbare Stückliste (Software Bill of Materials)

Habe ich ein vollständiges Lizenzmanagement?
die eigene Lizenzwahl und die der Vorproduzenten

SerNet

Werkzeuge für Lizenzprüfung und SBOM

Open Source

selbst betreiben, im Build automatisieren

REUSE Lizenz und Copyright je Datei prüfen

ScanCode Lizenzen und Copyrights im Code finden

ORT Abhängigkeiten, Lizenzen, Berichte

FOSSology Lizenz-Scans für Compliance-Teams

Syft, Dependency-Track SBOM-Werkzeuge

Kommerziell

Lizenz- und Schwachstellen-Management

Black Duck umfangreiche Lizenz-Wissensbasis

FOSSA Lizenz-Compliance, Attributionsberichte

Mend.io Lizenz- und Sicherheitsanalyse

Snyk Schwachstellen im Entwickler-Workflow

Sonatype Richtlinien direkt am Repository

Auswahl ohne Wertung. SBOM-Formate: SPDX, CycloneDX. REUSE hätte die OpenPAQ-Lücke gemeldet.

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Open-Source-Lizenz = Quellcode-Lizenz

Wortmarke `Wort` → Schriftzug | Logo | Bild

geschützt in jeder Verbildlichung

OSS-Lizenz `Quellcode` → Binary | Paket | Container

Lizenz gilt für jedes Kompilat

SerNet

Wer hat Anspruch auf den Quellcode?

Binary erhalten = Anspruch auf Quellcode

Wer das Binary hat, kann den Quellcode verlangen.

Kein Binary = kein Recht auf Quellcode

Wer nichts bekommen hat, kann auch nichts verlangen.

Kein Zwang zur Veröffentlichung

Weder Code noch Binary müssen öffentlich sein – Beispiel NIVADIS.

Besitz und Eigentum

Empfänger werden nicht nur Besitzer, sondern auch Eigentümer an Code und Binary.

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Recht zur Weitergabe – aber auch Pflichten

- Header unverändert beibehalten
- Eigene Änderungen: sich ggf. mit eintragen
- Die Pflichten reisen mit dem Code

```
/*
 * Copyright (C) 2019 Erika Mustermann
 * Copyright (C) 2026 Max Beispiel
 *
 * SPDX-License-Identifier:
 *     AGPL-3.0-or-later
 */
```

Gute KI wie Claude trägt den Autor mit ein und baut saubere Header – siehe vna web.

SerNet

vna web: KI trägt den Autor mit ein

veo-vna-importer / web/src/test/groovy/org/veo/importer/web/VeoInstanceUrlsTest.groovy

```
1  /*
2   * verinice.veo vna-importer
3   * Copyright (C) 2026  Johannes Loxen
4   *
5   * This program is free software: you can redistribute it and/or modify
6   * it under the terms of the GNU Affero General Public License as published by
7   * the Free Software Foundation, either version 3 of the License, or
8   * (at your option) any later version.
9   *
10  * This program is distributed in the hope that it will be useful,
11  * but WITHOUT ANY WARRANTY; without even the implied warranty of
12  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
13  * GNU Affero General Public License for more details.
14  *
15  * You should have received a copy of the GNU Affero General Public License
16  * along with this program.  If not, see <http://www.gnu.org/licenses/>.
17  */
18 package org.veo.importer.web
```

Quelle: veo-vna-importer · …/web/VeoInstanceUrlsTest.groovy

Copyright: Person

Zeile 3: Johannes Loxen, 2026

Lizenz: AGPLv3+

Zeilen 5–8, wie im ganzen Projekt

Haftungsausschluss

Zeilen 10–13: WITHOUT ANY WARRANTY

SerNet

Die wichtigsten Dateien im Repository



LICENSE

Vollständiger Lizenztext – nicht nur der Name



README

Was ist das Projekt, wie baut und nutzt man es?



SECURITY

Wie melde ich eine Schwachstelle?



NOTICE

Urheber, Drittkomponenten, Hinweise



Beispiel: `github.com/SerNet/verinice-veo`

SerNet

Vier Header im Vergleich

Beispiel	Projekt · Sprache	Copyright bei	Lizenz	Haftungsausschluss
Nasrallah	verinice-veo · Java	Person	AGPLv3 oder später	✓ im Header
Jordan	verinice-veo · Groovy	Person	AGPLv3 oder später	✓ im Header
Bartlett	Samba · C	Person	GPLv3 oder später	✓ im Header
Catalyst	Samba · Python	Firma (+ „Written by“)	GPLv3 oder später	✓ im Header

Gemeinsam: Copyright-Zeile, Lizenzhinweis und **`WITHOUT ANY WARRANTY`** – in jeder einzelnen Quelldatei.

SerNet

Persönliches Copyright, AGPL

SerNet / verinice-veo / veo-rest/src/main/java/org/veo/SpringPropertyLogger.java

```
1  /*
2   * verinice.veo
3   * Copyright (C) 2020  Alexander Ben Nasrallah.
4   *
5   * This program is free software: you can redistribute it and/or modify
6   * it under the terms of the GNU Affero General Public License as published by
7   * the Free Software Foundation, either version 3 of the License, or
8   * (at your option) any later version.
9   *
10  * This program is distributed in the hope that it will be useful,
11  * but WITHOUT ANY WARRANTY; without even the implied warranty of
12  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
13  * GNU Affero General Public License for more details.
14  *
15  * You should have received a copy of the GNU Affero General Public License
16  * along with this program.  If not, see <http://www.gnu.org/licenses/>.
17  */
```

Quelle: github.com/SerNet/verinice-veo · …/SpringPropertyLogger.java

Copyright: Person

Zeile 3: Alexander Ben Nasrallah, 2020

Lizenz: AGPLv3+

Zeilen 5–8, „or any later version“

Haftungsausschluss

Zeilen 10–13: WITHOUT ANY WARRANTY

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Gleiche Vorlage, anderer Autor

SerNet / verinice-veo / veo-rest/src/restTest/groovy/org/veo/jobs/RestTestDomainTemplateCreator.groovy

```
1  /*
2   * verinice.veo
3   * Copyright (C) 2022  Jonas Jordan
4   *
5   * This program is free software: you can redistribute it and/or modify
6   * it under the terms of the GNU Affero General Public License as published by
7   * the Free Software Foundation, either version 3 of the License, or
8   * (at your option) any later version.
9   *
10  * This program is distributed in the hope that it will be useful,
11  * but WITHOUT ANY WARRANTY; without even the implied warranty of
12  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
13  * GNU Affero General Public License for more details.
14  *
15  * You should have received a copy of the GNU Affero General Public License
16  * along with this program.  If not, see <http://www.gnu.org/licenses/>.
17  */
```

Quelle: github.com/SerNet/verinice-veo · …/RestTestDomainTemplateCreator.groovy

Copyright: Person

Zeile 3: Jonas Jordan, 2022

Lizenz: AGPLv3+

Zeilen 5–8, identisch im Projekt

Haftungsausschluss

Zeilen 10–13, wortgleich

SerNet

Persönliches Copyright, GPL

samba-team / samba / source3/auth/auth.c

```
1  /*
2     Unix SMB/CIFS implementation.
3     Password and authentication handling
4     Copyright (C) Andrew Bartlett         2001-2002
5
6     This program is free software; you can redistribute it and/or modify
7     it under the terms of the GNU General Public License as published by
8     the Free Software Foundation; either version 3 of the License, or
9     (at your option) any later version.
10
11    This program is distributed in the hope that it will be useful,
12    but WITHOUT ANY WARRANTY; without even the implied warranty of
13    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
14    GNU General Public License for more details.
15
16    You should have received a copy of the GNU General Public License
17    along with this program.  If not, see <http://www.gnu.org/licenses/>.
18 */
```

Quelle: gitlab.com/samba-team/samba · …/auth.c

Copyright: Person

Zeile 4: Andrew Bartlett, 2001–2002

Lizenz: GPLv3+

Code von 2001/02, Header seit 2007 auf GPLv3

Haftungsausschluss

Zeilen 11–14: WITHOUT ANY WARRANTY

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Firmen-Copyright, Autor genannt

samba-team / samba / python/samba/domain/models/auth_policy.py

```
1  # Unix SMB/CIFS implementation.
2  #
3  # Authentication policy model.
4  #
5  # Copyright (C) Catalyst.Net Ltd. 2023
6  #
7  # Written by Rob van der Linde <rob@catalyst.net.nz>
8  #
9  # This program is free software; you can redistribute it and/or modify
10 # it under the terms of the GNU General Public License as published by
11 # the Free Software Foundation; either version 3 of the License, or
12 # (at your option) any later version.
13 #
14 # This program is distributed in the hope that it will be useful,
15 # but WITHOUT ANY WARRANTY; without even the implied warranty of
16 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
17 # GNU General Public License for more details.
18 #
19 # You should have received a copy of the GNU General Public License
20 # along with this program.  If not, see <http://www.gnu.org/licenses/>.
21 #
```

Quelle: gitlab.com/samba-team/samba · …/auth_policy.py

Copyright: Firma

Z. 5: Catalyst.Net Ltd. – Z. 7: Autor als „Written by“

Lizenz: GPLv3+

Zeilen 9–12

Haftungsausschluss

Zeilen 14–17 – auch die Firma schließt aus

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Cyber Resilience Act: die Lieferkette wird Pflicht

10.12.2024
CRA in Kraft getreten

11.09.2026
Meldepflichten gelten

11.12.2027
Alle Pflichten gelten

Komponenten kennen

Hersteller prüfen eingebaute Drittkomponenten – auch Open Source (SBOM).

Schwachstellen melden

Aktiv ausgenutzte Lücken und schwere Vorfälle sind meldepflichtig.

Open-Source-Stewards

Eigene, leichtere Rolle; nicht-kommerzielle Entwicklung ist ausgenommen.

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Der CRA-Fahrplan für verinice

1 Einordnen

Produkt mit digitalen Elementen, kommerziell bereitgestellt → Herstellerpflichten

2 Anforderungen

Anhang I: 13 Produkt- und 8 Schwachstellen-Anforderungen als Checkliste

3 Risiko bewerten

Cyber-Risikobewertung, Supportzeitraum, Drittkomponenten prüfen

4 Nutzer informieren

Anhang II: Kontaktstelle, Supportende, Sicherheitshinweise

5 Konformität nachweisen

Modul A, technische Doku, EU-Konformitätserklärung, CE

6 Betreiben & melden

Meldepflichten, Marktüberwachung, 10 Jahre aufbewahren

Methode: *Checkliste je Abschnitt – Rechtsgrundlage, Status, Nachweis*

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Einordnen, Anforderungen, Risiko

Einordnen

- Software mit direkter Datenverbindung zu Geräten oder Netzen
- Open Source, aber per Subscription vertrieben → Hersteller
- Weder „wichtig“ (Anhang III) noch „kritisch“ (Anhang IV) → Standardkategorie

Anhang I

13 **Produktanforderungen**

secure by default, Updates, Zugriffsschutz, Verschlüsselung, kleine Angriffsfläche

8 **Schwachstellen-Prozesse**

SBOM, CVD-Policy, Meldeadresse, kostenlose Security-Updates

Risiko & Fristen

≥ 5 Jahre
Supportzeitraum

10 Jahre
jedes Security-Update verfügbar halten

Due Diligence für Drittkomponenten: Lücken an den Upstream melden und selbst beheben

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

SerNet

Nachweis: von der Doku zum CE-Zeichen

Technische Doku

Anhang VII: Beschreibung, Architektur, SBOM, CVD-Policy, Risikobewertung

→

Interne Kontrolle

Modul A (Anhang VIII): Hersteller prüft selbst – keine benannte Stelle

→

EU-Konformitäts-erklärung

Anhang V, oder vereinfacht (Anhang VI) mit Link auf die volle Fassung

→

CE-Kennzeichnung

Bei Software: auf der Erklärung oder auf der Produkt-Website

Nutzerinformation (Anhang II): zentrale Kontaktstelle für Schwachstellen, Supportende (Monat/Jahr), sichere Inbetriebnahme, Updates, Außerbetriebnahme, ggf. Fundort der SBOM

10 Jahre
Doku und Erklärung aufbewahren – oder länger, wenn der Support länger läuft

© 2026, SerNet GmbH · DENIC Spark · 10.11.2026

// Schritt 6 · gilt seit 11.09.2026

Melden: Die Uhr läuft ab Kenntnis

Aktiv ausgenutzte Schwachstelle	**24 h** Frühwarnung	→ **72 h** Schwachstellen-Meldung	→ **14 Tage** Abschlussbericht nach verfügbarer Abhilfe
Schwerer Sicherheitsvorfall	**24 h** Frühwarnung	→ **72 h** Vorfallsmeldung	→ **1 Monat** Abschlussbericht nach der Meldung

Meldeweg: über die zentrale Meldeplattform der ENISA an das koordinierende CSIRT und zugleich an die ENISA – und betroffene Nutzer informieren. Gilt auch für Produkte, die schon auf dem Markt sind.

Kontakt



Fragen? Diskussion!

Dr. Johannes Loxen

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen

Tel. +49 551 370000-0
Fax +49 551 370000-9

www.sernet.de
kontakt@sernet.de