#BFOS10: OpenSource-Software selbstbewusst verkaufen

Abstract:

"Selbstbewusst OpenSource-Software verkaufen - wie man typische Vertragsfallen umgeht."
Am Beispiel des Lieferkettengesetzes und der NIS-2 sowie an immer wieder auftauchenden Forderungen nach Vertragsstrafen behandelt der Vortrag, wie man als kleine und mittlere Anbieterin von Freier Software und Dienstleistungen im Machtspiel mit großen Kundinnen den eigenen Standpunkt behaupten und Verträge ohne diese Fallstricke abschliessen kann. Wenn noch Zeit ist und wenig Fragen kommen, geht der Vortrag noch auf Forderungen nach Versicherungen gegen DSGVO-Vorfälle ein oder die EVBIT-Cloud und C5-Katalog.

Hinweis zum Genus/Gendern: Firmen sind meistens weiblich („die Gesellschaft“), also schreibe ich fast durchgehend von Kundinnen. Die Kunden („der Verband“) sind aber immer mit gemeint :-)

Vortrag:

Dem Vortrag selbst stehen nur 20 Minuten inkl. Fragen zur Verfügung, so dass dort nur kursorisch gesprochen kann. Dieser vorliegende Text bietet die Möglichkeit, die einzelnen Gesetze etwas tiefer im Detail zu beleuchten und die Vor- und Nachteile einzelner Gesetze und üblichen Vertragsbedingungen insbesondere aus dem Blickwinkel von OpenSource-Software („OSS“) zu betrachten.

LkSG: Lieferkettensorgfaltspflichtengesetz

Seit 1.1.2024 gilt das Gesetz für Unternehmen mit mehr als 1000 Beschäftigten. Davor galt es für Unternehmen mit mehr als 3000 Beschäftigten. Kleinere, nicht betroffene Unternehmen leiden seit diesem Jahr darunter, dass die Betroffenen versuchen, Verpflichtungen abzuwälzen, die sie nicht abwälzen dürfen. Jede Form der pauschalen Verpflichtung und Verantwortungsübergabe an nicht Betroffene ist im Gesetz explizit verboten, das BFA hat dazu eine sehr gute Handreichung geschrieben: https://www.bafa.de/DE/Lieferketten/FAQ/haeufig_gestellte_fragen_node.html und die Abschnitte 17.3 und 17.5. sollten von nicht betroffenen Firmen gut durchgelesen werden.

Wir bei SerNet haben unzählige Aufforderungen von großen Kundinnen erhalten, die uns pauschal verpflichten wollten und uns damit ohne Ende Arbeit aufgehalst hätten, wenn wir uns nicht immer rigoros gewehrt und die Zusammenarbeit abgelehnt hätten. Wir haben unsere Kundinnen immer darauf hingewiesen, dass sie eine Risikoanalyse selber machen müssen und mit einem dann evtl. gefunden **konkreten** Risiko auf uns zukommen sollen und wir dann natürlich gerne helfen – und dies auch müssen. Unsere Kundinnen schickten uns oft Links zu Portalen, auf denen wir uns einloggen und komplexe Fragebögen ausfüllen sollten – oftmals nur mit Ja/Nein-Antworten, die beide falsch sind, wenn uns eine Frage nicht betrifft, was aber meistens keine Antwortoption war.

Oft stand schon am Anfang des Fragebogens, dass die Nicht-Teilnahme Nachteile bei späteren Aufträgen zur Folge haben könnten. Diesen Firmen haben wir dann direkt ein Zitat aus der BAFA-Hilfestellung geschickt, dass dies ungesetzlich ist und zur Anzeige gebracht werden kann.

Es kann schon sein, dass wir durch unsere Verweigerungshaltung Aufträge verloren haben und ich habe auch zB bei der IHK eskaliert, dass das Gesetz auch für nicht Betroffene starke Nachteile hat – aber wir sind hier selbstbewusst und haben objektiv keine Nachteile bei Beauftragungen feststellen können. Wir haben uns auf jeden Fall viele Stunden und Tage an Arbeit gespart und vor allen

Dingen Assessments, deren Antworten uns später vielleicht Schwierigkeiten machen. Meistens ist beim LkSG „keine Antwort“ besser als „irgendeine Antwort“.

Was hat das mit OSS zu tun? Wenn es nicht um Dienstleistungen der SerNet ging (die wir immer ohne Unterauftragnehmer leisten und damit also wenig Probleme haben), sondern um unsere Software-Produkte SAMBA+ oder verinice, haben wir unsere anfragenden Kundinnen immer auf unsere zukünftige Verpflichtung nach dem **CRA** (siehe unten) hingewiesen: Wir liefern für unsere Programme bereits jetzt „Software Bill of Materials“, sogenannte **SBOM**. Dank einer Initiative der Linux Foundation aus 2011 gibt es mit SPDX einen offenen Standard für Lieferketten-Verwaltung in Software. GitHub erledigt dies für unsere Web-Anwendung **verinice** sogar voll automatisch.

Wenn uns also ein Kundin eines Tages mit einem konkreten Risiko kommt, können wir unsere Lieferkette in einem offenen Repository einfach nachweisen und bei der Risiko-Mitigation aushelfen.

NIS-2: Netz- und Informationssicherheitsrichtlinie, Version 2 aus 2023/2024

Die NIS-2 hat nicht direkt mit OSS zu tun. Ich erwähne sie aber, weil sie im Richtlinien-Tandem mit der CRA kommt. Von NIS-2 sind mittlere/große Firmen betroffen, die die im Gesetz benannten Dienste im Internet leisten, also zum Beispiel Cloud-Dienste anbieten oder Managed Services. Domain-Registrare sind sogar völlig ohne Rücksicht auf die Größe immer betroffen, also evtl. auch die kleine Werbeagentur mit 3 Mitarbeitenden. Wir bei SerNet sind als mittleres Unternehmen genau hier betroffen: Wir hosten den Cloud-Dienst „veo.verinice.com“, wir erbringen „Managed Security Services“ auf den Firewalls unserer Kundinnen und registrieren für diese auch Domains.

Die Anforderungen der NIS-2 sind aber überschaubar, siehe dazu meinen anderen Vortrag unter loxen.de/nis2.pdf. Die eigenen Systeme mit Firewalls nach dem Stand der Technik zu schützen und ein überprüfbares Schwachstellenmanagement vorweisen zu können, wenn tatsächlich etwas schwerwiegendes passiert und die Aufsichtsbehörde (in Deutschland das BSI) zu Besuch kommt, sind die ja durchaus umsetzbaren Minimalforderungen der NIS-2 und wer auf OSS im Betrieb setzt und selbst Dienste auf Basis von OSS anbietet, hat im Prüfungsfall ein klares Transparenz-Plus.

CRA: Cyber Resilience Act

Während sich die NIS-2 auf Dienste im Internet bezieht, will sich der CRA um die Qualität von Software kümmern und hier hat OSS meines Erachtens deutlich die Nase vorn, auch wenn man sich natürlich nicht über jede neue Regulierung freut. Nur echte nicht-kommerzielle Software-Aktivität ist nicht vom CRA betroffen. Wer OSS verkauft, Support leistet oder nur entfernt mit OSS Geld verdient, muss sich um die Sicherheit dieser Software kümmern. Wichtig ist, dass man automatisch alle Verantwortlichkeiten für eine Software erbt, wenn man sie sich zu Eigen macht. Neben der Pflicht des Inhalts- und Herkunftsnachweises über **SBOM** kommen jede Menge Sorgfaltspflichten bei der Planung, Erstellung, In-Verkehr-Bringung, Pflege und Wartung aus dem CRA auf Herstellerinnen zu.

Natürlich hat kommerzielle OSS hier keine Sonderstellung, denn sie hat spezifische eigene Sicherheits-Risiken, die proprietäre Software nicht hat (z.b. die Gefahr der Brunnenvergiftung von freien Quellen). Andererseits hat sie den Vorteil der hausgemachten Transparenz und damit die Chance auf öffentliche Automatisierung, siehe zum Beispiel die automatische Erstellung von SBOM bei GitHub:

Den/das/die SBOM von verinice kann man zB direkt hier herunterladen, nachdem man sich bei GitHub angemeldet hat: https://github.com/SerNet/verinice-veo/network/dependencies.

DS-GVO: Datenschutz-Grundverordnung

Die DSGVO hat erst einmal nichts mit OSS zu tun – auch wenn auf dem Univention Summit im Januar ein Sprecher in seinem Vortrag behauptete, dass nur mit OpenSource datenschutzkonforme Software möglich sei, was Unsinn ist. (Der gleiche Sprecher sagte, dass OSS „gemeinfrei“ sei und in der „Public Domain“, was aber nicht das gleiche ist.)

Warum ich hier dennoch auf den Datenschutz eingehe, sind pauschale Vertragsstrafen für Datenschutzvorfälle, die wir immer wieder in Verträgen finden. Kundinnen wollen sich so die Arbeit ersparen, bei Datenschutzvorfällen einen Schadenersatz auszurechnen, der zudem oft nicht-materieller Natur oder nur schwer zu beziffern ist. Pauschale Strafen, die dann „pro Vorfall“ gelten, sind leichter einfordern, wenn sie im Vertrag vereinbart wurden. Diese stellen aber ein beträchtliches Risiko dar, denn 1.000 Euro Strafe pro Vorfall sind üblich – und wer in einer Marketingmail an 1.000 Empfängerinnen einen Datenschutzfehler macht, sieht sich evtl. einer Forderung von 1.000.000 Euro ausgesetzt. Durch die lange oft auch nachvertragliche Geltungsdauer solche Regelungen hat man schnell sehr gefährliche Zeitbomben im Vertragsportfolio.

Wir haben bei SerNet seit Gründung jeden Vertragsentwurf von Kundinnen und jede AEB/AGB mit pauschalen Vertragsstrafen abgelehnt und nicht ein einziger Vertrag kam deshalb nicht zu Stande. Dies geschieht bei uns ca. 4x im Jahr. Alle Vertragspartner haben dann dieses Passus gestrichen.

Cyberversicherungen decken in diesem Zusammenhang vertragliche und Prozess-Risiken ab, aber weder kommen diese für freiwillig akzeptierte Vertragsstrafen auf noch für Bußgelder, die nach festgestellten Datenschutzvorfällen dazu kommen können.

EVB-IT: Ergänzende Vertragsbedingungen IT

Seit über 20 Jahren gestalten wir bei SerNet unsere Verträge für Lieferungen und Leistungen mit den AGB der Öffentlichen Hand: den EVB-IT. Da Allgemeine Geschäftsbedingungen immer ein Machtkampf sind und es darum geht, welcher Vertragspartner es einfacher hat, wenn er seine bereits geprüften Bedingungen durchsetzen kann, statt die Bedingungen des Partner zu prüfen, ist es hilfreich, wenn man als kleines/junges Unternehmen ein AGB-Werk nimmt, das von objektiv-dritter Seite kommt und das die Kundin in der Regel schon kennt, weil sie oft selbst auch für die Öffentliche Hand arbeitet.

Schon immer sind die EVB-IT für Lieferungen und Leistungen von OSS sehr gut geeignet.

Ich gehe im weiteren noch genauer darauf ein. Momentan (September 2024) arbeiten wir in einer Arbeitsgruppe des Bitkom zusammen mit den zuständigen Bundesministerien an einer noch besseren Integration von OSS in die EVBIT-Verträge. Hier geht es aber oft um Details wie saubere Benennung und Rahmenbedingungen, die den Vertrags-Juristinnen wichtig sind :-)

EVB-IT Software-Überlassung Typ A/B: Mit nur sehr wenig Aufwand kann man Subskriptionen für OSS mit diesen AGB vertraglich gestalten. Typ A bezieht sich auf „dauerhafte“ und Typ B auf „befristete“ Überlassung und Nutzung. SerNet nimmt Typ A, weil man unsere OSS auch nach Ende der Subskription dauerhaft nutzen kann (anders als zum Beispiel bei RedHats „Enterprise Linux“, die harte vertragliche Klimmzüge machen, um die Nutzung nach Abo-Ende zu unterdrücken). Manche unserer Kundinnen bestehen auf Typ B, weil sie die zeitlich begrenzte Subskription im Vordergrund sehen und die unbegrenzte Nutzung sowieso nicht in Anspruch nehmen dürfen („kein Softwareeinsatz ohne Support“) – das soll der SerNet dann auch sehr recht sein :-)

Wichtig ist, dass nichts in den Überlassungs-EVB gegen OSS als Vertragsgegenstand spricht.

EVB-IT Dienstleistungen: Das schöne an diesen AGB ist, dass sie rechtlich sauber und gleich zu Beginn die Ergebnisverantwortung des Auftraggebers bei Dienstleistungen benennt, denn der Auftragnehmer/Dienstleister schuldet „nur“ den Aufwand nach Stand der Technik und schuldet nicht das Ergebnis. Nur auf dieser Vertragsbasis kann man ad-hoc in Support bei der Kundin eintreten, ohne erst ein Pflichtenheft zu erstellen und Margen zu kalkulieren für den Fall, dass man ein Problem nicht gelöst bekommt. Dies wird mit Kundinnen ja oft diskutiert, die nicht bezahlen wollen oder Abschläge verlangen, wenn ein Support-Ergebnis nicht wie gewünscht eintritt.

Gerade bei OSS, wo sich die Kundinnen ihre Software „sonstwo.com“ herunter geladen haben, ist es wichtig, dass die Dienstleisterin voraussetzungsfrei in die sofortige Arbeit eintreten kann. Dazu sind diese EVB eine hervorragende vertragliche Unterstützung und wir bei SerNet nutzen sie bei einer StartUps genauso wie beim Großkunden – wenn dieser uns nicht seine AEB aufzwingt :-)

EVB-IT Cloud: Diese AGB sind ein eher staatliches Geschenk an Großkonzerne, denn zusätzlich zur Verpflichtung auf den Betrieb von Cloud-Diensten nach den Vorgaben der „ISO 27001“ oder des „BSI IT-Grundschutzes“ (die man im Mittelstand noch gut schaffen kann) steht dort auch die Verpflichtung auf den BSI-Katalog C5 – und der ist durch kleinere Firmen nicht zu schaffen und durch große Mittelständler auch nur mit viel Aufwand. Wer also seine OSS zB als SaaS – „Software as a Service“ selber anbieten will, kann dies für Kunden aus der Öffentlichen Hand kaum selber betreiben, sondern wird dies immer mit Partner umsetzen. Diese AGB müssen wir also an dieser Stelle aus OSS-Sicht kaum betrachten – aber vielleicht doch noch ein paar Details zum C5:

C5: Cloud Computing Compliance Controls Catalogue des BSI

Die Anforderungen des C5-Katalogs sind extrem, zum Beispiel bei der Inventarisierung und Buchhaltung aller verwendeten Hardware inklusive ihrer Entsorgung. Aus Deutschland gibt es derzeit nur wenige Anbieter, die dies unterstützen: zB T-Systems, Hetzner, IONOS, PlusServer und Noris Network. Viele Anbieterinnen mit C5-Angebot sind in der Hand ausländischer Firmen und aus Sicht der digitalen Souveränität mit Vorsicht zu betrachten:

Der Bitkom berichtet in seiner Pressemeldung, dass 39% der im Vorjahr gemeldeten Cyberangriffe mutmaßlich aus Russland kommen und sogar 45% aus China. Entsprechend vorsichtig/abwehrend ist zB das BSI bei russischen Software-Anbietern (siehe Kaspersky) und chinesischen Ausrüstern (siehe Huawei). Auf der gleichen Bitkom-Folie stehen aber auch 25% Angriffe aus den USA. Mit einer NSA, die Wirtschaftsspionage im Staatsauftrag hat, sollte man also auch bei US-Anbietern vorsichtig sein, die C5 anbieten, aber keine echte Souveränität für Kundinnen in Deutschland und Europa anbieten können (Microsoft, AWS, Google etc.).

Naturgemäß ist der Bitkom als Verband der IT-Unternehmen „in“ Deutschland (und nicht „aus“ Deutschland), der auch die Mitgliedsbeiträge aller Mitglieder gerne annimmt, in dieser Sache kein objektiver Ratgeber. Es wäre also zu wünschen, dass Einrichtungen wie das ZenDIS, der „Sovereign Techfund“ und andere staatlich finanzierte Einrichtungen, die sich für mehr digitale Souveränität einsetzen, noch mehr Aufmerksamkeit bekommen.

Fazit:

Es ist nicht die schlechteste aller Zeiten, um sich vertragssicher für mehr OpenSource-Software und digitale Souveränität in Deutschland und Europa einzusetzen. Man kann dies auch als kleines und mittleres Unternehmen selbstbewusst tun, wenn man sich vernetzt und vertretbare Risiken eingeht.

SerNet

Selbstbewusst OpenSource-Software verkaufen

10. Bitkom Forum Open Source - 12. September 2024

Dr. Johannes Loxen

SerNet GmbH, Göttingen – Berlin – San Francisco

Exposé: loxen.de/bfoss24.pdf

SerNet GmbH, SerNet, Inc.

SerNet

- gegründet 1997, Büros in Göttingen und Berlin
- Tochterfirma „SerNet, Inc.“ in San Francisco
- Schwerpunkt Informationssicherheit und Datenschutz
- Produkte und Dienstleistungen rund um Sichere Infrastruktur
  - Firewalls, VPN, E-Mail, Archivierung, Virtualisierung, Hybride Cloud, M365
- verinice.: Open Source ISMS-Tool für Informations-Sicherheits-Management
- SAMBA+: Open Source Alternative zu Windows-Servern, IAM
- Klassischer Mittelstand: private Hand, kein Risiko-Kapital, keine Kredite
- über 5000 Bestandskunden in Deutschland, Europa, USA und weltweit

Gesetze und Bedingungen

SerNet

NIS 2

Ergänzende Vertragsbedingungen IT

Lieferkettensorgfaltspflichtengesetz

DS-GVO

C5

Cyber Resilience Act

Netz- und Informationssicherheitsrichtlinie

CRA

LkSG

Cloud Computing Compliance Controls Catalogue

Datenschutz-Grundverordnung

EVB-IT

Kontakt

SerNet

Dr. Johannes Loxen, jl@sernet.de

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen

tel +49 (551) 370000-0

http://www.sernet.de
kontakt@sernet.de

SerNet, Inc.
101 Montgomery St, #1900
San Francisco CA 94104

+1 (415) 248-7818

http://www.sernet.com
contact@sernet.com