DORA: Open Source gegen Closed Source

(IT-Regulierung: DORA: Regulierung für die Finanzbranche; iX 3/2024, S. 58)

Im Artikel „DORA: Neue Regulierung für mehr Resilienz in der Finanzbranche“ schreiben Sie: „So ist Quellcode von Dritten und proprietäre Software auf Verwundbarkeiten und Anomalien zu überprüfen. Ob es damit für Finanzunternehmen noch möglich sein wird, Open-Source-Software zu verwenden, ist eine spannende Frage.“

Mich würde interessieren, wie Sie zu der Schlussfolgerung kommen, dass der Einsatz von Open-Source-Software durch diese DORA-Regulierung fraglich sein könnte. Genau betrachtet, können regulierte Unternehmen diese Vorgabe ausschließlich für Open-Source-Software umfänglich erfüllen. Denn nur dort ist es ihnen möglich, mittels diverser Techniken und Tools (beispielsweise statische/dynamische Codeanalyse, Code-Reviews etc.) den tatsächlichen Quellcode zu prüfen, entsprechende Nachweise zu generieren und gefundene Verwundbarkeiten und Anomalien gegebenenfalls sogar selbst zu beheben oder zumindest an die Entwickler direkt oder indirekt zu melden.

Im Bereich der Closed-Source-Software kann eine entsprechende Prüfung auf technischer Ebene (fast) nur durch einen Schwachstellenscanner erfolgen, der allerdings Verwundbarkeiten und Anomalien nur erkennt, wenn diese bereits dem Hersteller und/oder öffentlich bekannt sind. Das heißt, regulierte Unternehmen müssen auf entsprechende Vertragsklauseln ausweichen, um die Anforderung auf organisatorischer Ebene zu erfüllen, da davon auszugehen ist, dass die technische Ebene unzureichend ist. Und wird es nicht genau an dieser Stelle erst spannend?

Es ist wohl davon auszugehen, dass kein Softwarehersteller eine Vertragsklausel aufnimmt, die dem regulierten Unternehmen attestiert, dass die Closed-Source-Software frei von Verwundbarkeiten und Anomalien ist. Fraglich ist auch, ob die Softwarehersteller entsprechende Nachweise liefern werden (beispielsweise in Form von Test- und Auditprotokollen oder einer Dokumentation über das Vorhandensein eines Secure Software Development Lifecycles) – man denke insbesondere an die sehr großen Hersteller.

SEBASTIAN BECKER, VIA E-MAIL

Vielen Dank für Ihre Rückmeldung. Grundsätzlich gibt es zu DORA viele spannende Fragen und im Rahmen der Umsetzung (die einzelnen Aspekte stehen ja noch gar nicht final fest) werden sich mit Sicherheit noch weitere Fragen ergeben.

Ich gebe Ihnen vollkommen recht, dass bei Closed-Shop-Software viele Anforderungen nur vertraglich geregelt werden können. Vermutlich ging es dem Gesetzgeber auch darum, dass die Anforderungen aus DORA, insbesondere hinsichtlich IKT-Drittdienstleistern, nicht mit Open-Source-Software umgangen werden.

Im finalen Draft zum technischen Regulierungsstandard IKT Risikomanagement (muss formal noch durch das EU-Parlament beschlossen werden) steht unter anderem Folgendes in Artikel 16, 2. (f): „The requirement that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment.“

Ich kann Ihnen nicht sagen, wie viele Finanzunternehmen DORA erfüllen müssen. In unserer Finanzgruppe handelt es sich um über 700 Kreditinstitute, wie im Artikel erwähnt sind dabei auch sehr kleine Institute. Und für Kreditinstitute gibt es leider auch keine Ausnahmeregelungen.

Der direkte Draht zu

Direktwahl zur Redaktion: 0511 5352-387

Redaktion iX | Postfach 61 04 07
30604 Hannover | Fax: 0511 5352-361
E-Mail: post@ix.de | Web: www.ix.de

www.facebook.com/ix.magazin
twitter.com/ixmagazin (News)
twitter.com/ix (Sonstiges)

Für E-Mail-Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion gern zur Verfügung.

Listing-Service:
Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/

Große Konzerne wie Allianz oder die Deutsche Bank haben eventuell die Expertise, um diese Anforderung aus DORA zu erfüllen. Bei den in Deutschland überwiegend mittelständisch geprägten Finanzunternehmen wage ich das zu bezweifeln.

Vielleicht bietet auch der neu hinzugefügte Halbsatz „where feasible“ neue Handlungsspielräume.

(Thomas Mayerhoffer)

Vom FeRD erzählt

(Kolumne: Trojanisches ZUGFeRD; iX 3/2024, S. 11)

Die Kritik, dass nicht auf der technischen Ebene spezifiziert ist, wie mit inhaltlich korrupten Nachrichten im ZUGFeRD-Protokoll umzugehen ist, in denen die beiden inhaltlich redundanten XML-Teile (in der PDF und separat) voneinander abweichen, ist durchaus berechtigt.

Aber die Schlussfolgerung daraus ist falsch. Es liegt nämlich im Interesse des Rechnungsstellers, darauf zu achten, dass das nicht passiert. Eine Rechnung, bei der es da Abweichungen gibt, ist formal inkorrekt. Dann liegt der Verdacht nahe, dass sie gefälscht sein könnte. Im Interesse der Verhinderung illegaler Zahlungen sollte sie dann nicht beglichen, sondern zurückgewiesen werden. Der Rechnungssteller verliert damit nur Zeit, bis er sein Geld erhält. Das wäre also Selbstschädigung. Also ist im System klar ein Interesse beider Seiten enthalten, auf die (formale) Korrektheit der ZUGFeRD-XML-Nachrichten und insbesondere die Übereinstimmung der Daten dieser beiden XML-Informationen genauso zu achten wie auf die Übereinstimmung der Daten der PDF-Darstellung mit dem XML-Anteil. Auch hier würden Abweichungen einen Fehler darstellen, der zur Zurückweisung der Rechnung berechtigen würde.

Insofern ist es ganz einfach, wenn Abweichungen der XML-Passagen beziehungsweise Inkonsistenzen in der Rechnung Kopfzerbrechen verursachen würden. Den anderen muss man nichts vom FeRD erzählen.

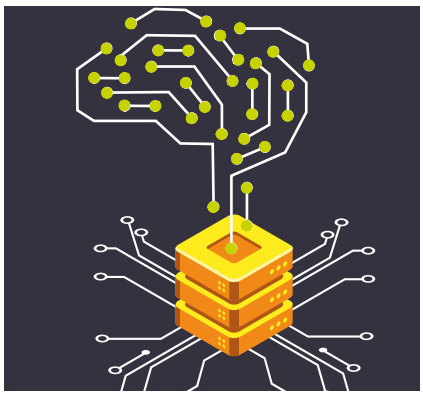
GERHARD ROLAND, VIA E-MAIL

Informativer, anregender Artikel

(Machine Learning: Von HPC lernen – ML im Rechenzentrum; iX 4/2024, S. 54)

Sehr anschaulich und dennoch nicht flach. Erhellende Erkenntnisse mit konkreten Beispielen und auch Zahlen. Brotkrumen als mögliche Ausgangspunkte für eigenständige Weiterrecherche auch reichlich vorhanden. Super!

AXEL SIODELSKI, AUS DEM IX-FORUM



Backups ohne Tricks

(Sicherheitskonferenz: Kontraproduktiv: Viele Opfer von Cybercrime halten sich bedeckt; iX 3/2024, S. 8)

Vielen Dank für den super Artikel. Dazu noch eine Frage zu den erwähnten Air-Gap-Backups: Was muss man sich darunter vorstellen? Offsite gelagerte Tapes?

HARRY BUNTZ, VIA E-MAIL

Lieben Dank für das gute Feedback. Zu Ihrer Frage: Wenn ich von echten Air Gaps spreche, sind in meinen Augen damit sämtliche „Online-Tricks“ kategorisch vom Tisch. Bandwechsler verbieten sich ebenso wie jegliche Onlinedatenspeicher, damit ist auch Immutable-Speicher gemeint. Ebenso verbietet sich jeder Cloud-Speicher, es sei denn, der Cloud-Anbieter selbst verkauft einem zusätzlich die logistische Leistung einer definierten manuellen Auslagerung. Air Gap bedeutet aus meiner Sicht also Daten, welche streng „kalt“, also jenseits von jeder denkbaren Elektronik, die online darauf zugreifen könnte, gelagert sind. Das können selbstverständlich Tapes sein, müssen es aber nicht zwangsläufig. *(Jörg Riether)*

Die iX-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.