Digitale Souveränität durch Open Source

Unabhängigkeitserklärung

Dr. Gerhard Weck

Das Umstellen auf Open Source ist eine Aufgabe, die das Gemeinschaftsgefühl in der EU stärken könnte. Zudem würde es die Abhängigkeit von bestimmten Anbietern deutlich reduzieren. Politik und Wirtschaft sind gefordert.

Von vielen Entscheidern im IT-Bereich unbemerkt oder bewusst ignoriert, hat sich in den letzten Jahren die Entwicklung und der Einsatz von IT-Systemen auf wenige Hard- und Softwarebasissysteme verengt. Häufig heißt es, die Beschränkung auf wenige Produkte, die angeblich miteinander besonders kompatibel seien, vereinfache die Arbeit, und außerdem sei das notwendige Fachpersonal leichter verfügbar. Alternative Hard- und Software wird bei der Planung und Beschaffung oft nicht einmal in Betracht gezogen, selbst wenn sie aus betrieblicher, ökonomischer und sicherheitstechnischer Sicht überlegen ist.

Die Software der meisten heute eingesetzten Systeme basiert auf wenigen Betriebssystemen und Anwendungspaketen, die zu einem großen Teil als Closed Source angeboten werden (Abbildung 1, siehe ix.de/zq7k). Damit ist es nicht möglich, das korrekte Funktionieren bis auf die Ebene des Quellcodes zu überprüfen und zu bewerten. Und durch nicht erkannte Lücken und Hintertüren können vertrauliche Daten abfließen oder manipuliert werden. Außerdem können Angriffe auf zentrale, weithin genutzte Komponenten, wie kürzlich bei Exchange geschehen, zu weitreichenden, kaum zu behebenden Schäden führen (siehe ix.de/zq7k). Großflächige Ausfälle – es sei an Emotet erinnert – zeigen die Dringlichkeit. Insbesondere der weitverbreitete Einsatz der Telemetrie, über die viele Daten an den Hersteller gelangen, sowie der Zwang zum Aktivieren erworbener Lizenzen durch explizite Freischaltung können den völligen Verlust der Kontrolle über die eingesetzte Software nach sich ziehen.

Etliche politische Akteure sehen Erpressung, Vertragsbruch und gezielte Attacken auf Firmen mit dem Ziel, sie aus dem Markt drängen, als normal an. Es besteht die Gefahr, dass politischer Druck einzelne Hersteller zwingt, ihre Produkte aus bestimmten Ländern zurückzuziehen oder deren Lauffähigkeit dort zu beschränken. Es ist auch möglich, dass manche Anwendungen sich schlicht nicht mehr verwenden lassen. Das kann viele Gründe haben, zum Beispiel könnte der Anbieter aus dem Markt verschwunden sein, die Pflege aufgegeben oder Funktionen und Lizenzierung so geändert haben, dass das Produkt für seinen bisherigen Zweck nicht mehr infrage kommt oder nicht mehr legal eingesetzt werden darf.

Da die betreffende Hard- und Software ausschließlich aus Nicht-EU-Ländern stammt, besteht eine starke Abhängigkeit von anderen Staaten, aus der die EU nicht herauskommt, solange es hier keine äquivalente Fertigung gibt. Das ist besonders dann kritisch, wenn in einem bestimmten Bereich ein Hersteller eine Monopolstellung hat, weil er seinen Kunden fast beliebige Bedingungen diktieren und damit sogar deren Wirtschaftlichkeit unterminieren kann.

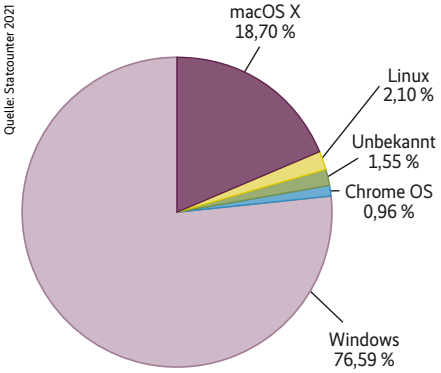
EU muss eigenständiger werden

Der Ausfall von IT-Komponenten eines Anbieters kann volkswirtschaftlich katastrophale Folgen haben, wenn keine Möglichkeit besteht, schnell und mit tragbarem Aufwand auf vergleichbare Produkte umzusteigen. Insbesondere für Systeme der öffentlichen Hand und für kritische Infrastrukturen (KRITIS, siehe ix.de/zq7k) ist dieses Risiko inakzeptabel. Dennoch zeigt die derzeitige Entwicklung bei den zentralen Softwarekomponenten die Tendenz, dass sich Abhängigkeiten von einzelnen Anbietern noch verstärken. Eine angemessene Wirtschaftspolitik und der Aufbau und Ausbau eigener Hard- und Softwareherstellung in Deutschland und der EU könnte eine echte digitale Souveränität gewährleisten.

Nur eine eigenständige europäische Entwicklung und Produktion sicherer Hard- und Softwaresysteme wird – vollständig dokumentiert und von allen Anwendern nachvollziehbar – unerwünschte Eingriffe ausschließen. Insbesondere sind die fol-

genden Vorgehensweisen bei kritischen Infrastrukturen einschließlich Systemen der öffentlichen Hand (Bund, Länder, Kreisebene, Gemeinden) und allgemein beim Verarbeiten personenbezogener Daten unter Beachtung der Datenschutz-Grundverordnung (DSGVO) unabdingbar und durch die jeweiligen Bedarfsträger bei Neu- und Weiterentwicklungen zu gewährleisten:

- Auf der Ebene der Betriebssysteme muss ein systematischer Übergang von Closed Source zu Open Source stattfinden. Nur solche Systeme bieten die Chance, unabhängig von bestimmten Herstellern und deren politischer Umgebung zu agieren. Dadurch ließe sich auch sicherstellen, dass die Betroffenen beim Ausfall eines Lieferanten schnell und mit überschaubarem Aufwand auf ein anderes System umsteigen können. Doch auch bei Open-Source-Komponenten muss die Pflege dauerhaft sichergestellt sein.
- Sofern übergangsweise, etwa aus Gründen funktionaler Mängel bestimmter Open-Source-Produkte, noch ein Parallelbetrieb mit den bisher eingesetzten Closed-Source-Systemen erforderlich ist, müssen Letztere in einer abgeschotteten Umgebung ohne Internetzugriff laufen, um einen unkontrollierten Datenabfluss zu verhindern. Gleichzeitig ist die Entwicklung einer funktional vollständigen Open-Source-Alternative voranzutreiben.
- Auch bei den Anwendungssystemen, etwa Office-Paketen, müssen die Verantwortlichen den Übergang auf Open-Source-Pakete vorsehen und dabei offene Standards einhalten (Abbildung 2).



Desktop-Betriebssysteme in Europa: Den Platzhirsch Microsoft zu verdrängen, dürfte die EU noch einige Mühe kosten (Abb. 1).

Statt proprietärer Datenformate sollten unbedingt standardisierte Formate wie ISO 26300 (Open Document Format for Office Applications) zum Einsatz kommen. Sofern hier noch Abhängigkeiten zu Closed-Source-Produkten bestehen, müssen geeignete Migrationsstrategien entwickelt und kurzfristig umgesetzt werden.

- Unzureichende Funktionen einzelner Open-Source-Komponenten dürfen nicht das Ausweichen auf herkömmliche Closed-Source-Produkte zur Folge haben, sondern die fehlenden Funktionen müssen ergänzt werden.
- Software, die in kritischen Bereichen läuft und rechtlichen Rahmenbedingungen wie dem IT-Sicherheitsgesetz oder der DSGVO unterliegt, muss hinreichend bis auf Quellcode-Ebene auf ihre Sicherheit geprüft sein.

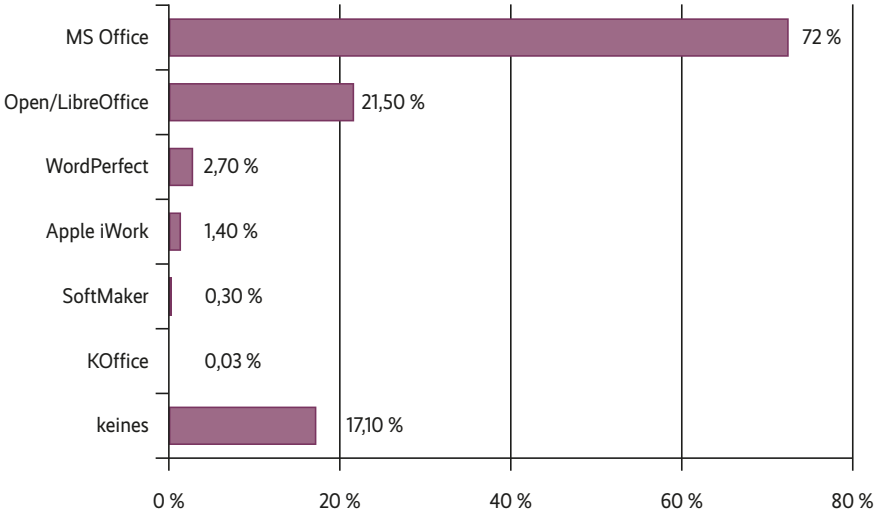
Diese Forderungen widersprechen zum Teil den bei Beschaffung und Nutzung von Software üblichen Praktiken, die häufig vorrangig das Ziel der Risikominimierung durch Fortschreibung der bisher eingesetzten Systeme ohne Prüfung möglicher Alternativen verfolgen. Man sollte jedoch den hier beschriebenen Ansatz nicht vorschnell als unpraktikabel oder gar weltfremd abtun, da die in der Praxis – zum Beispiel bei Zertifizierungen – vorgefundenen Systeme häufig gravierende Mängel aufweisen, vor allem hinsichtlich ihrer Sicherheit und der datenschutzrechtlichen Anforderungen.

Vieles verstößt gegen geltendes Recht

Die geplante IT-Modernisierung des Bundes, die auf Windows 10 setzt und sich möglicherweise über die nächsten zehn Jahre hinzieht, ist völlig inakzeptabel (siehe ix.de/zq7k). Das vielfach vorgebrachte Argument – beispielsweise bei dem Münchner Schwenk von LiMux zu Windows –, dass gerade wegen der Abhängigkeit vieler Fachanwendungen von den bisher eingesetzten Closed-Source-Umgebungen keine wirtschaftliche Migration auf Standards und Open Source möglich sei, ist meist nur vorgeschoben und kaschiert lediglich den mangelnden Willen oder sogar die Unfähigkeit, langfristige Strategien zu entwickeln und umzusetzen (siehe ix.de/zq7k).

Daher sind die folgenden Vorgehensweisen unabdingbar:

- Fachanwendungen müssen grundsätzlich vom eingesetzten Betriebssystem unabhängig sein. Dies lässt sich beispielsweise durch den Einsatz webbasierter



Nutzung von Office-Produkten in Deutschland: Auch hier ist Microsoft immer noch weit vorn, obwohl es eine gute Alternative gibt (Abb. 2).

Anwendungen erreichen, die es erlauben, eine Applikation unabhängig von der technischen Ausstattung des Endanwenders zu nutzen.

- Ausschreibungen für Fachanwendungen müssen klarstellen, dass diese in Open-Source-Umgebungen laufen müssen, um die geforderte Transparenz sicherzustellen. Die Einschränkung auf proprietäre Umgebungen ist als negatives Bewertungskriterium oder sogar als Ausschlusskriterium zu sehen. Inakzeptabel wäre etwa, wenn öffentliche Ausschreibungen schon die Software eines Monopolisten vorgeben.
- Weitverbreitete Fachanwendungen im Behördenumfeld sind, unter Bezug auf offene Standards, ein einziges Mal zu entwickeln und dann allgemein zur Verfügung zu stellen, beispielsweise über das geplante Code Repository der Kollaborativen Freien Softwareplattform für Verwaltungen der Free Software Foundation Europe (FSFE) (siehe ix.de/zq7k). Es ist wirtschaftlich nicht vertretbar, dieselbe Anwendung mehrfach entwickeln zu lassen, nur um einige lokale Anforderungen abzudecken. Stattdessen sind Letztere als Optionen in der allgemein verfügbaren Anwendung zu entwickeln und bereitzustellen.
- Heikel sind die vielen „inoffiziellen" Mini-Fachanwendungen, die oft in Nacht-und-Nebel-Aktionen entstehen, um spezifische operationelle Probleme ad hoc zu lösen. Es handelt sich beispielsweise um Excel-Tabellen oder kleine Access-Anwendungen, die zwischen Fachabteilungen ausgetauscht werden, um spezielle Anforderungen abzudecken, die die großen, „offiziellen" Fachverfahren nur unzureichend erfüllen. Solche Minianwendungen sind oft nicht oder nur unzureichend dokumentiert, sodass es schwierig sein kann, sie zu ersetzen. Aus Sicht der IT-Sicherheit und des Datenschutzes ist es jedoch geboten, an diesen Stellen aufzuräumen und derartige Schwachstellen zu entfernen, da gerade hier oft die vorgegebenen Regularien verletzt werden, ohne dass es (außerhalb einer Zertifizierung) groß auffällt.

Für eine begrenzte Zeit lassen sich noch nicht auf offene Standards umgesetzte Fachanwendungen in abgeschotteten Umgebungen bis zur vollständigen Migration tolerieren. So kann man beispielsweise Windows-Systeme ohne Weiteres als virtuelle Maschinen in Open-Source-Umgebungen betreiben, zumal die gängigen Virtualisierungsumgebungen wie VMware, VirtualBox oder Qubes OS den Datenaustausch zwischen den virtuellen Gastsystemen und den zugrunde liegenden Hosts problemlos abwickeln.

Auch die weitverbreitete Telemetrie in vielen Produkten, bei der nicht überprüfbare Datenmengen zum – möglicherweise außereuropäischen – Hersteller abfließen, ist nicht datenschutzkonform, insbesondere nachdem der Rechtsrahmen des Privacy Shield dies nicht mehr abdeckt. Folglich widerspricht der Einsatz populärer Programme zum Verarbeiten personenbezogener Daten oft den Vorgaben der DSGVO, die eine explizite Einwilligung der Betroffenen verlangt. In der Regel gibt es keine praktikable Möglichkeit, hier zu widersprechen.

Entwicklung und Pflege von Open Source ist, wie jede Entwicklung, mit Aufwand und Kosten verbunden. Die hier geforderte Nutzung solcher Software muss diese Situation berücksichtigen, indem der Abnehmer der IT-Dienste das Entwickeln und Pflegen geeigneter Komponenten finanziell und durch Bereitstellen der notwendigen Kapazitäten explizit fördert.

Wege aus der Umklammerung

Dabei bietet sich für Europa die Chance, die Abhängigkeit von den USA und anderen außereuropäischen Ländern zu verringern, indem es Open-Source-Projekte, die heute schon zu einem nicht unerheblichen Teil von Entwicklern in Europa betreut werden, direkt fördert, beispielsweise durch die Unterstützung beim Schließen funktionaler Lücken. Statt, wie es jetzt noch häufig der Fall ist, solche Lücken zu bemängeln und deshalb auf Closed-Source-Produkte auszuweichen, ist dieses Vorgehen zielführender. Statt erhebliche Summen als Lizenzgebühren an außereuropäische Hersteller zu zahlen, wäre eine Investition in das Erstellen und Weiterentwickeln hiesiger Anwendungen sowohl volkswirtschaftlich zweckmäßiger als auch förderlich für die digitale Souveränität Europas.

Auch heute gibt es schon eine Reihe von Open-Source-Projekten, die ganz oder zu einem großen Teil auf europäischen Entwicklungen basieren. Dazu gehören bei den Betriebssystemen der L4-Systemkern, ReactOS und Qubes OS, bei den Virtualisierungstechniken VirtualBox und Xen, bei den datenschutzfreundlichen Techniken GNU Privacy Guard, Tails und Whonix sowie bei der Anwendungssoftware LibreOffice.

Allein die Tatsache, dass man ad hoc eine solche Liste von Open-Source-Projekten benennen kann, zeigt, dass Europa über konkrete Möglichkeiten verfügt, sich zumindest zum Teil aus externer Abhängigkeit zu befreien. Dies könnte einen signifikanten Wettbewerbsvorteil bringen, doch benötigen diese Projekte wesentlich mehr Unterstützung aus Politik und Wirtschaft sowie eine bessere Finanzierung.

(jd@ix.de)

Quellen

Weiterführende Informationen unter www.ix.de/zq7k

Dr. Gerhard Weck

ist IT-Sicherheitsberater und Mitglied im Präsidiums-Arbeitskreis „Datenschutz und IT-Sicherheit" bei der Gesellschaft für Informatik.