

DER TAGESSPIEGEL



Software Colony Europe

All European states use software from Microsoft in their administrations – and are making themselves ever more dependent on the US corporation. Why that is so risky – technically and politically. BY HARALD SCHUMANN AND ELISA SIMANTKE



The Microsoft logo PHOTO: THOMAS HAWK/FLICKR

When the Munich city council convenes, then it's not usually of much interest to anyone outside the city limits. But on this February day everything was different. Every one of the seats for members of the press and spectators was occupied in the big hall of the magnificent, neo-Gothic city hall. Those who couldn't find a seat were standing in the aisles. Council members reported they had received e-mails and media enquiries from all over Germany and Europe.

And yet the occasion seemed to be purely technical. For 10 years, experts were busy converting the city's IT system to free and open software. The expensive programmes of the US corporation Microsoft are now only used in exceptional cases. That not only saved a double-digit million sum in licence fees, but also made the system more secure – “a great success”, as the city government announced in 2014. But now City Mayor Dieter Reiter and his grand coalition of centre-left Social Democratic Party (SPD) and centre-right Christian Social Union (CSU) want to go back to Microsoft with all the city's 24,000 office computers.

There was a fierce debate. Mr. Reiter and his supporters couldn't give cogent reasons – nor could they say how much it would cost. So the decision had to be postponed. The head of the Green

parliamentary party Florian Roth was annoyed: it seemed to be nothing more than a “political power game,” he said, but a highly risky one. He added the warning, “do we really want to make our administration eternally dependent on the American monopolist Microsoft?”

In the whole of Europe, the IT in state administrations is based on Microsoft programmes

The question is by no means exaggerated, and it isn't restricted to Munich. In the whole of Europe, from Finland to Portugal, from Ireland to Greece, information technology (IT) in state administrations is based on programmes of the US software corporation. But because digital systems continue to grow and become ever more important, the states become increasingly more dependent on this one company. The EU commission even conceded that it was “in effective captivity with Microsoft.”

What are the consequences of this “lock-in” to one supplier, as it is called in technical jargon? And how can governments deal with it? The team of journalists from Investigate Europe went on a three-month fact-finding mission, interviewing economists, IT managers, security experts and politicians in 12 European countries, as well as the EU commission and Parliament. The results are disturbing.

The states' dependence on Microsoft

- creates steadily increasing costs and blocks technical progress in state authorities;
- systematically undermines European procurement and competition law;
- brings with it a stifling political influence from the corporation;
- and puts state IT systems along with the data of their citizens at a high technical and political security risk.

Microsoft was unwilling to answer any of Investigate Europe's questions about these issues. And public IT administration insiders know why.

“Many state administrations are so dependent on this one supplier that they no longer have a choice about which software to use. That means European states are in danger of losing control over their own IT infrastructure,” warned computer scientist and lawyer Martin Schallbruch, who up until 2016 was head of the department for information technology and cyber security in the German Federal Ministry of the Interior and is only too familiar with the precarious situation. If this danger is to be averted and a “switch made to independent IT architecture” it would require “enormous investment” said the experienced IT manager, who now does research at the Berlin business school ESMT.

But the problem is not just acute, it is also complex. At the core of the matter is Microsoft's business model. The software giant from Redmond in the US State of Washington sells its software, above all, the operating system Windows and the office programmes Word, Excel, Powerpoint and Outlook as licenced products. And the corresponding programme code remains secret (see box). This

“proprietary” form of software, as it is called in industry jargon, prevents possible competitors being able to use their own software to properly present all the data produced by Microsoft programmes. That means headlines, tables or dates suddenly looking different and “formatting” lost. Every computer user has experienced the phenomenon.

That is the key for the global monopoly of Microsoft – and what a fabulous business it is. Year after year the corporation pulls in some \$50 billion in licence fees just for distributing programme copies. And because colleagues, business partners and friends communicate using Microsoft files, it makes sense to do the same thing, even if fees are incurred – again and again. Even most users of Apple computers buy Microsoft’s Office suite.

Administrative authorities are at the mercy of Microsoft

And the state IT administrators are fully aware of this. This monoculture has serious disadvantages. In other sectors, the software development has long adhered to a completely different principle. Google or Siemens, for example, work primarily with “open source” programmes, i.e. software, the source code of which they share openly. That means every programmer and every firm can use them, but the latter in turn have to make every improvement they make accessible to the public. That means companies cannot earn money by selling software like this, but at the same time, they benefit from the work of programmers all over the world without having to pay for it.

Siemens needs comprehensive software packages for all products from power stations to x-ray machines. But 90 percent of them perform standard tasks, as the computer scientist Karsten Gerloff from the department responsible within the company explained. “And for these of course we use open source solutions.” The company only uses a “proprietary code” for special functions unique to Siemens machines. But if all software had to be written by the company’s own staff, “we would have to employ an additional 1,000 programmers and would no longer be competitive,” said Mr. Gerloff.

Naturally, the participation of many creative minds all over the world produces a greater dynamic than the restriction to one company. That is why “open source is now the standard in science and business,” said Matthias Kirschner, President of the Free Software Foundation Europe (FSFE), who argues in favour of self-determination dealing with information technology. That applies just as much to smartphones as it does to supercomputers, machine control systems and web servers. The old monopoly only still applies to desktop and office software.

As a consequence public administration authorities still rely on the same old monopoly and not just for office programmes. There are thousands of special applications, which only authorities need. Whether taxes are to be increased, pensions paid or waste collection charges calculated - in the police, social welfare or building authorities; for nearly every service the state provides, there is software in operation, especially developed for the task. But because the Windows operating system is used

everywhere, all these “special applications” are based on this system – putting the authorities at the mercy of the manufacturer.

Just how far this goes, was shown when at the end of 2014 Microsoft stopped delivering security updates for the “Windows XP” version. Suddenly state institutions right across Europe saw themselves forced to enter into expensive service contracts with Microsoft, so the company would continue to close security gaps in its old programme. The British government paid €6.5 million for one extra year time to adapt its computers to “Windows 7”. The Netherlands also paid several million euros for an extension, as did Germany’s lower Saxony and Berlin. “The same thing happened all over Europe,” confirmed an expert at the EU Commission. This state of affairs threatens to continue in three years’ time when the updates for Windows 7 are also terminated.

The EU Commission ignores its own experts

At the same time, states are falling behind because of the lock-in with Microsoft. “There is no firm evidence to prove this yet, but it is logical to assume that the dependence on one supplier is slowing down technical progress in the public sector,” warned Dietmar Harhoff, Director of the Max-Planck-Institute for innovation and competition in Munich. If, for example, the municipalities were to develop their many hundred special programmes on an open source basis, then every innovation could immediately be used by all the other city administrations without additional costs. “This potential is enormous for the public sector,” said Mr. Harhoff.

As early as 2012 the EU Commission thus launched a programme with the demonstrative title “Against lock-in”. The idea was that in all future state tenders for the purchase of information technology and software no brand names of companies or their proprietary technical standards would be used. Instead, public institutions would only ask for the fulfilment of “open standards” which would be accessible for every manufacturer. If it came to this, then Microsoft’s monopoly would disappear in time, because there would be no more problems with compatibility – files would also be readable with competing products and without any loss of data. If all administrative authorities were to use the same open formats, then all would save the licence fees. “Open standards create competition, lead to innovation and save money,” explained the then Commissioner for Competition Nellie Kroes. “The lack of competition” in the IT sector “costs the public sector alone €1.1 billion per year,” her experts calculated.

But the lethargy of state bureaucracy was greater than all the good intentions, and the initiative came to nothing. And yet EU law sets clear rules here. Central government authorities have to put out to public tender in the whole of Europe all orders worth more than €135,000. For all other public corporations that applies to a volume of €209,000. When they are buying standard software for their administration, Europe’s governments collectively just override this valid law in favour of the traditional, preferred supplier Microsoft.

Bizarre processes instead of competition

And to do this, there is a bizarre process. Without any tender they negotiate discounts with the US corporation and conclude framework contracts on that basis. All public corporations can then sign up. In subsequent tenders, they only look for dealers who will sell them Microsoft licences according to these conditions. De facto there is no competition for such public contracts.

That's how it is in Germany too. In 2015 the Federal Ministry of the Interior (BMI) agreed new "condition contracts" with the Irish branch of Microsoft, from where the corporation runs its European business tax-efficiently. The discounts named in the new agreement can be taken up by all authorities, from a federal ministry to a small municipality. In one tender, for example, the city of Dortmund was then only looking for a "retail partner for the Microsoft volume licence contract BMI."

That is like the state issuing a tender to buy motor cars, but only from Volkswagen dealers, says the Dutch lawyer Matthieu Paapst mockingly. For his Ph.D. at the University of Groningen he investigated software procurement by the public sector. His conclusion: "The practice of procuring Microsoft products for public administration without an open tender violates valid EU law." And actually, according to Mr. Paapst, the EU Commission should take action against it. The only reason that is not happening is because the EU authority itself is not observing the correct practice.

The EU Commission does indeed have an exclusive contract with Microsoft, which is valid for all EU institutions – and thus ignores the recommendations of its own experts. This is also "completely legal" claims Gertrud Ingestad, head of the responsible Director General for Computer Science (DG Digit) in an interview with Investigate Europe. There would be "no other possibility" of guaranteeing the continuity of the EU's work. And in such a case the law explicitly permits a non-public "negotiation process". But that is not correct. This exception is explicitly valid "only when there is no reasonable alternative or replacement solution," as stated in article 32 of the relevant EU guideline. And exactly that is what Director General Ms. Ingestad and her colleagues cannot prove. There are viable alternatives.

The Italian general Camillo Sileo, for example, has a lot to say on that subject. The officer works in Rome's military district and receives visitors in a small lecture room. There he speaks with a soft voice and a smile about his project as if it was just a small matter. But he heads up the unusual, almost revolutionary operation "Libre Difesa", Free Defence. His objective is to convert to open source software the entire Italian army's roughly 100,000 office computers. "We have discovered that for our purposes, both programmes are equally good," the general explained. "Just look," he said and pointed to the projection of the front page of a recently conducted study by his ministry. "There you can see it as a file from Microsoft Word," he said and clicked again. "And here is the open source LibreOffice version. Coat of arms, headline, structure, everything is there, no difference," he said happily. "The migration will save €28 million by 2020," General Sileo promised. In crisis-ridden Italy, the Army too has to save.

The fact that the conversion has run smoothly so far is because of good planning, according to the general. The alternative programme can do everything, but it has to be operated in a different way, and therefore users have to be trained. For this to happen, volunteers of the open source movement “Libre Italia” have trained members of all military services as trainers and advisers, who in turn have trained further colleagues themselves. There should soon be enough experts at all army locations. The precondition for success is “good communication,” General Sileo assured: “If people understand the reason, then they overcome any mental resistance.” Whether the army will also convert the operating system one day and become completely independent of Microsoft, has not yet been decided. But that will be “looked into thoroughly,” said General Sileo.

The French “Gendarmerie Nationale”, one of France’s two national police forces, has already completed this conversion process which began as early as 2005. Now there are 72,000 state police computers with an individually adapted version of the free operating system Linux plus LibreOffice as the main application. The authority claims that by 2014 it had already saved around €20 million. However, up to that point, the so-called “migration” was implemented practically in secret. “The change to Linux could be seen by Microsoft as a threat to its monopoly,” was the text of an internal memo, which Investigate Europe has obtained. And that could “lead” to “actions aimed at discrediting this policy of the gendarmerie.” That is why the change had to ensue “without publicity”, until “the process” was “irreversible.”

Institutions put under pressure which opt out

This caution was justified. Even today, 12 years after the launch of the project, the leadership of the gendarmerie is still under “permanent pressure” to turn back, reported a staff member of the IT department of the Interior Ministry in Paris, who did not wish to be named for fear of sanctions. “Every day their system works is a slap in the face of our administrators, who maintain that only Microsoft functions properly,” he said.

The power struggle of the ministries with Linux fans in the police force is confirmed by a letter from the ministry in April 2016, which Investigate Europe has seen. In it, the ministry calls for the officers responsible of the gendarmerie to finally revert to Windows completely - an instruction which the leadership of the police has not carried out to this day. When asked about the matter, a spokesperson “regretted” they were “unable to give any information.” At the same time, though, he wrote in a discernibly subversive tone that the conversion to free software “took place quietly and sustainably,” and “we chose Linux because it makes us more cost-efficient and ultimately independent.”

The conflict is indicative of a phenomenon experienced everywhere by pioneers wanting to opt out of the monopoly. All over Europe there have been and still are hundreds of authorities and municipalities, which have changed to open source software, or have attempted to do so. From the state pension authority in Sweden to schools in Polish Jaworzno to the city administration of Rome, from the London borough of Camden to the big French city of Nantes to the regional government in Spain’s

Extremadura, or the Portuguese city of Vieira do Minho. All these projects are to this day islands in the Microsoft ocean, and for that reason are repeatedly put under pressure to conform, because both the products and lobbyists of Microsoft are ubiquitous and can always create new problems.

Lobbyists work directly in ministries

That is also a factor behind the scenes in the dispute about the Munich city administration. There the centre-left SPD mayor needs the votes of the centre-right CSU. But the latter is closely linked with the US corporation. Dorothee Belz, for example, who was a vice president at Microsoft Europe until 2015 and is a member of the executive committee of the conservative party's economic council.

Similar revolving door episodes can be found all over Europe. In Italy a former Microsoft manager now controls the "digital transformation" of the business metropolis Milan. In Portugal a Microsoft executive managed the election campaign of the conservative president. In France the corporation has as many as six managers and advisers with close connections to ministries and politicians. At the same time, technical employees of Microsoft work directly in the government's IT administration. At least five of them have e-mail addresses, identifying them as government staff members, which enable them to "do lobby work for Microsoft directly in the administration," as an official confirmed to Investigate Europe. In Germany access to government computers is wide open too. There are several thousand external experts in government computer centres, including people from Microsoft and their partners, reported the former federal government IT head Martin Schallbruch.

The corporation can also instrumentalise schools and universities for its marketing without restriction. Schoolchildren and teachers usually receive Microsoft products free of charge, so that children grow up knowing nothing else. After all their studies, the calculation is that they will pay licence fees for the rest of their life. It is the classic "crack model" as every drug dealer uses it, says Rufus Pollock of the Centre for Intellectual Property and Information Law (CIPIL) at the University of Cambridge. They get the stuff free of charge until they are hooked.

All that demonstrates is that Europe's governing bodies give tacit approval to their dependence on Microsoft, or as Anna Strezynska, Poland's minister for digitalisation, puts it, "yes, we are dependent, but I think that is reasonable."

But it means they are exposing their states and their citizens to an incalculable security risk – technically and politically.

It is by no means a coincidence that all major hacker attacks of recent years on state institutions like the German Bundestag, the EU Commission or the European Parliament all took place via security gaps in Microsoft programmes. The office software of Microsoft in particular and the files it produces are the most important gateway for cyberattacks. That is what the Federal Office for the Security of Information Technology (BSI) reported back in 2011. According to the report half of all "targeted attacks" were perpetrated by infected documents in Microsoft formats like "docx", in which the

attackers concealed their malware. This was made easier by the particular complexity of these files according to the BSI experts. They contain much more code than would actually be necessary, not least of all to make them more difficult to read for other programmes. “That statement remains valid,” confirmed BSI spokesman Joachim Wagner. The format of Microsoft files is “considerably more complex” than that of open source programmes and offers the attacker a correspondingly bigger target,” Mr. Wagner explained.

One of the experts behind the free office programme LibreOffice, Italo Vignoli, put it to the test for Investigate Europe with a simple text of 5,500 characters. In the current version of “Microsoft Word” the code contained in the relevant file fills 390 pages. By contrast, in the open format “OpenDocument Text” it fills just 11 pages.

Microsoft programmes are complex and vulnerable

The special vulnerability of Microsoft’s office programmes is reflected in the number of its security gaps. For “Microsoft Office” the American “National Institute for Standards and Technology” reported 188 newly registered “exploits” in the three years leading up to April 2017, three quarters of which were in the worst category. In the same period only 11 security gaps were discovered for LibreOffice. This had nothing to do with it being distributed far less widely, according to Mr. Vignoli. It was simply that - despite all their efforts - even top experts were unable to find any additional security gaps.

And that is not surprising. After all, the code it is based on can be checked by any knowledgeable operator. This is where Michael Waidner, director of the Fraunhofer Institute for secure information technology and one of the leading European experts, sees the key. “If the state or the European Union really want to be sovereign entities, they have to be in a position to test whether the hardware and software of its information technology only do what they are supposed to do and nothing else,” said Mr. Waidner. That doesn’t mean Europe has to become self-sufficient. “But we have to insist that our experts have all the information they need to test the software in security-sensitive areas. Access to the source code is essential,” the leading expert demanded. Without it there is “no digital sovereignty.”

And that is exactly what Microsoft refuses to provide. The company did set up a “transparency centre” in Brussels where government representatives are given an opportunity to inspect the code. But Germany’s BSI dismissed the offer as inadequate. “Comprehensive technical preconditions” would have to be met in order “to create an atmosphere of trust,” the BSI explained to the trade magazine “C’t”. But Microsoft did not even allow to take written notes out of the room and demands to sign a non-disclosure agreement, a BSI expert confirmed to Investigate Europe. And even if an examination were possible, it might no longer be valid after the next programme update. Because the Microsoft products are not just technically, but also politically risky.

That is because the corporation is subject to American law. So it can be forced at any time to help the US authorities access the data of foreign authorities or citizens. For that purpose there is the so-called “National Security Letter” in US law empowering secret courts to issue instructions of this nature, including the obligation to maintain confidentiality under penalty of law. The revelations of former agent Edward Snowden have shown that America’s secret services make extensive use of these powers. The documents published by him show that Microsoft co-operates closely with the secret service NSA.

For example, a NSA document of March 8, 2013 describes in detail that Microsoft even gave the US authorities access to the company’s “cloud” service, i.e. to those data storage facilities where an increasing number of firms and also state authorities outsource their IT to save the costs of having their own IT department. The Snowden documents also proved that the NSA used a cyberweapon called “Regin” in co-operation with its British partners to spy on the EU Commission and the European Parliament – via a security gap in the Windows programme.

Wikileaks has published secret documents which prove that this was no isolated case. They show that the CIA even developed a veritable tool kit of malware exclusively targeting Windows programmes. And so did the NSA, which contained even four different so far unknown security gaps for the Windows system (“zero day exploits”) revealed the hacker group “Shadow Brokers” recently.

De facto the use of Microsoft products in state authorities is “no longer compatible with a state under the rule of law,” said the lawyer and Green European Parliament member Jan Philipp Albrecht, who is considered by many to be the father of EU data protection law. He went on to say there was a plethora of personal data about citizens stored on state computers, including tax payments, state of health, police files and social data. “But the authorities cannot guarantee that these data remain private as long as they are working with software not under their control,” warned Mr. Albrecht. That would have to change, “otherwise we will downgrade Europe to a digital colony.”

Mr. Albrecht is by no means alone in expressing such views. Back in 2014 after the Snowden revelations there was a big majority in the European Parliament calling for EU states to jointly “develop key autonomous IT capacities as a strategic measure” and that these would “have to be based on open standards and open source software,” so they “could be tested.”

A year later the newly elected parliament again called for a “European strategy for independence in the IT sector” And it indicated how this could be achieved: it was important to establish “a publicly accessible source code as a mandatory selection criterion in all public sector IT procurement procedures,” as called for by security researcher Michael Waidner.

If it came to that, Mr. Albrecht thinks it would have an effect on information technology “like an Airbus project.” Just like Europe once made itself independent of Boeing, it could also get over its dependence on Microsoft and at much lower cost: if open source became mandatory for standard

software then “Europe’s players would immediately be competitive,” promised Mr. Albrecht. After all, he added, the required alternatives have long been developed.

But up to now Europe’s governments don’t even know how high the states’ “tribute payments” are to their “licence masters” in Redmond, USA. The answer from the government departments responsible to enquiries made by Investigate Europe from Norway to Portugal was that there were no such statistics. The procurement office of the German Federal Ministry of the Interior also replied that they could only make an “estimate” of expenditure by federal authorities on Microsoft licences. But even 10 weeks after the enquiry was made, the authority was still unable to produce the data.

The IT market analysis company Pierre Audoin Consultants estimates that in Europe overall in the business year 2015/16 Microsoft generated revenues with the public sector of nearly €2 billion. That would mean that at least €20 billion of European tax revenues go to the U.S. corporation every decade – certainly enough for Europe to develop its own software industry.

But so far, Europe’s rulers don’t want to know anything about an Airbus project for the IT industry. Andrus Ansip, EU Commissioner for the digital single market, doesn’t even want to talk about it. His leading official, Director General Roberto Viola, played down the issue, saying it was “not our main concern.”

America’s internet corporations on the other hand, know better. Whether it is Facebook, Google or Amazon, they all operate their IT infrastructure exclusively with open source software, according to company spokesmen. Because that is the only way they can protect themselves. And that is exactly what China’s rulers want too. They started their liberation from the Microsoft monopoly after the NSA scandal. Under the leadership of the National Academy of Engineering the open operating system “Neokylin” was developed along with the corresponding office software. The “de-windowising“, as project manager Professor Ni Guangang calls it, will go ahead primarily in security-sensitive sectors. That is why the use of open programs is becoming mandatory for the military, government authorities and the financial sector, and the process is to be completed by the year 2020.

China is making itself independent. What is Europe doing?