Kommentar von außen

Warum es wichtig ist, dass Microsoft seinen Weg zu 100% OpenSource weiterverfolgt.

Auf Grund der aktuellen politischen Ereignisse in Österreich rund um die Digitalisierung der Bildung[1], durfte ich in den letzten Wochen und dank COVID-19, sogar Monaten, mich wiederholt reflektierend mit vielen Strömungen zur Umsetzung der Digitalisierung im Allgemeinen, im besonders sensiblen Bereich der Bildung im Speziellen, befassen.

Zusammenfassend: Open Source versus Microsoft versus Google versus Apple versus Amazon versus alles dazwischen.

Das schlimme an dieser Debatte ist nicht die Tatsache, dass sie stattfindet – die aktuelle Krise zeigt mehr denn je, dass dies bitter notwendig ist, sondern das „wie" diese Debatten geführt wird. Alle haben berechtigter Weise Angst auf das falsche Pferd zu setzen und somit (besonders im Bildungsbereich) Steuergeld der Bürgerinnen und Bürger zu verschwenden oder das eigene Unternehmens-Know-How aufzugeben bzw. auf bereits jetzt kaputte Geschäftsmodelle zu setzen. Das Thema Datenschutz im Bereich der Bildung ist nochmal mehr Herausforderung, da es beim Lernen mit digitalen Medien um einen hochsensiblen Bereich geht und wir hier die Daten unserer Schülerinnen und Schüler mindestens genauso gut schützen müssen, wie dies Banken machen im Bereich Online Banking.

Darum erlauben Sie mir, ein paar Jahre zurück in die Vergangenheit zu gehen, zu dem Zeitpunkt, als Satya Nadella das Ruder bei Microsoft in die Hand genommen hat:

Was war das Geschäftsmodell von Microsoft damals:

- Lizenzen verkaufen – für Betriebssysteme, Office Software, etc. und das auf möglichst vielen unterschiedlichen Plattformen, was man eben als Unternehmen leisten kann und rentabel ist.

Wie sahen die Geschäftsmodelle der Konkurrenz aus:

Google: wir verkaufen die Daten unserer privaten Kunden für Werbung, schließlich muss der Betrieb von G-Suite und vielen anderen Lösungen in Form von Rechenzentren und Infrastruktur gesichert sein und bauen parallel für Unternehmen bezahlte abgesicherte Lösungen.

Amazon: wir sind der beste und größte Logistikbetrieb der Welt, wir verdienen an der gesamten Supply Chain, damit wir skalieren können brauchen wir die beste IT, fast schon als Abfallsprodukt entstand AWS. Wenn man also Amazon effektiv besteuern möchte (abgesehen von Steuerschlupflöchern), bedarf es einzig und allein eines ordentlichen Mindestkollektivvertrags für die Logistikbranche und alle, die an dieser Supply Chain beteiligt sind.

Apple: wir liefern alles aus einer Hand – von der Hardware, zur Software zur Cloud – mit all den damit einhergehenden Vor- und Nachteilen unter Einhaltung wohl dokumentierter APIs.

Open Source: wir liefern Know-How und technischen Support – es läuft zwar so ziemlich alles was die Konkurrenz anbietet auf unseren Plattformen (Google, Facebook, Amazon, etc.), wir schaffen es allerdings insbesondere im Bereich Cloud noch nicht entsprechend zu skalieren. Eigentlich Paradox.

[1] https://www.bmbwf.gv.at/dam/jcr:78638403-697b-4b78-943b-9b9d2b20aa8f/Presseunterlage_PK_Digitalisierung_in_Schulen_20200617.pdf

Welche anderen Assets hatte Microsoft zu diesem Zeitpunkt eigentlich?

- Rechenzentren über die gesamte Welt verstreut
- Entwickler – nicht nur die im eigenen Haus, auch überall anders, da Visual Studio sich trotz der hohen Lizenzkosten, sich hoher Beliebtheit erfreute (und die Lizenzkosten, waren in Wahrheit ja auch nur für größere Unternehmen schlagend, da Microsoft es gerade durch das Partner Programm verstand den KMUs unter die Arme zu greifen)
- Akzeptierte Oberflächen, die besonders bei den Kunden gut ankamen (egal ob Windows oder Office, auch wenn Apple und Google hier sicherlich immer wieder andere Wege aufzeigten, so gab hier Microsoft den Ton an)

Welche zu erwartenden Damoklesschwerter bedrohten damals bereits die langfristige Existenz von Microsoft?

- DSGVO – auch wenn sie damals noch keinen expliziten Namen hatte, so gab es doch in vielen sensiblen Bereichen schon weitreichende Überlegungen zum Datenschutz. Interessanterweise gaben da einzelne Schulbezirke und Bundesstaaten in den USA insbesondere beim Einsatz von digitalen Endgeräten für Schülerinnen und Schüler besonders strenge Auflagen vor. Dies begünstigte Apple am US-Schulmarkt, andere Entwicklungen Google, sodass Microsoft im Bildungsbereich dasselbe Fiasko drohte, wie mit der Windows Mobile Plattform. Edward Snowden und die NSA halfen hier sicherlich für eine Beschleunigung und eine öffentliche Sichtbarkeit des Themas an sich.
- FOSS – Public money for public code – die Debatte wird besonders in Deutschland heiß geführt. Die Argumentation ist stringent und nachvollziehbar – für geschlossene Plattformen, ohne sauber dokumentierten Schnittstellen, wird es eng. Parallel kam es mit den Creative Commons und im Bildungsbereich mit OER (Open Education Ressources – Lerninhalte die jede Lehrperson an die Bedürfnisse der eigenen Klasse anpassen kann) auch im Content Bereich zu einem Umdenken. Hier ist Österreich mit den Plattformen eduthek.at und eduvidual.at und der Vergütung und Qualitätssicherung der erstellten Materialien durch das National Competence Center eEducation Austria anderen Ländern weit voraus. Brauchen wir deshalb keine Verlage mehr? NEIN! Wir brauchen Pluralität im System – einen Teil werden die klassischen Verlage, die sich mehr als besonnen auf die Digitalisierung vorbereiten und bereits umsetzen[2], leisten und einen anderen Teil, wird das System Schule durch die beteiligten Lehrpersonen dank OER auch selbst leisten. Digitalisierung ist exponentiell und muss skalieren können, all das muss bei jedem Schritt konsequent mitgedacht werden.

Als Satya Nadella das Ruder übernahm, gab es das legendäre Motto „Mobile first – Cloud first“. Plattformtechnisch hat man sich, trotz Übernahme von Nokia nicht halten können. Windows Mobile hatte viele Funktionen wie Live-Kacheln, die jetzt erst in die Designsprache von Apple in iOS 14 einfließen werden. Mit Windows 8 und der radikalen Änderung der Designsprache hat man viele Nutzer überfordert. Erst mit Windows 10 wurde begonnen konsequent zu Ende zu Denken.

Aber welches Ende wird das sein?

Mobile first – Cloud first kann nur dann funktionieren, auch in Zukunft, wenn man auf offene Standards setzt: Microsoft wandelte sich zu einem Open Source Unternehmen, mit Open Source Geschäftsstrategie. Natürlich funktioniert dies nicht von heute auf morgen, aber die Ankündigungen

[2] https://www.veritas.at/ahs.html

der letzten Ignite Konferenz im November erscheinen unter diesen Aspekt betrachtet nur eine logische Konsequenz zu sein.[3],[4]

Auszug aus der Open Source Geschichte von Microsoft:

1.) 2015 Visual Studio Code und .NET Core[5]
2.) 2015 Chakra – JavaScript Engine des Edge Browsers[6]
3.) 2016 Xamarin – Entwicklungsumgebung für mobile Endgeräte[7]
4.) 2016 PowerShell[8]
5.) 2016 Partnerschaft mit Canonical um Ubuntu auf Windows 10 zu bringen[9]
6.) 2018 Kauf von GitHub – die populärste Plattform für Entwickler*innen, um gemeinsam an Code zu arbeiten[10]

Doch dann kam der historische November 2019 – die oben bereits angesprochene Ignite Konferenz:

- Beginnend mit Windows 10 Version 2004 wurde ein vollwertiges Linux in Windows integriert und soll ausgebaut werden, dass auch sämtliche Linux Applikationen unter Windows ausgeführt werden können[11]
- Microsoft tauscht den Browser auf den 100% Open Source basierenden Chromium aus[12]
- Die beliebten PowerToys aus Windows 95/98 Zeiten werden gemeinsam mit der Community für Windows 10 neu aufgelegt[13]

Und zu guter Letzt: Microsoft Fluid Framework.

Das Fluid Framework ist Microsoft's Open Source Antwort um sich folgender Frage nicht mehr stellen zu müssen: Wenn wir jetzt alle auf Office 365 setzen, dann sind ja alle Daten bei Microsoft in der Cloud und ich kann unter Umständen vorhandene Legacy Apps und Plattformen wie Moodle gar nicht ordentlich integrieren – noch schlimmer – von dort wieder Rückportieren.[14]

Bleibt noch ein Aspekt ungeklärt: Datenschutz

Erlauben Sie mir das Thema in seine 2 Teilaspekte zu untergliedern:

---

[3] https://www.microsoft.com/en-us/microsoft-365/blog/2019/11/04/use-the-power-of-cloud-intelligence-to-simplify-and-accelerate-it-and-the-move-to-a-modern-workplace/
[4] https://searchvirtualdesktop.techtarget.com/opinion/Microsoft-Ignite-2019-news-Intune-SCCM-Endpoint-Manager-WVD-on-Azure-Stack-Hub-more
[5] https://github.com/Microsoft/vscode
[6] https://blogs.windows.com/msedgedev/2015/12/05/open-source-chakra-core/
[7] http://www.theverge.com/2016/2/24/11109942/microsoft-xamarin-acquisition-mobile-app-development
[8] https://blogs.msdn.microsoft.com/powershell/2016/08/17/windows-powershell-is-now-powershell-an-open-source-project-with-linux-support-how-did-we-do-it/
[9] http://www.theverge.com/2016/3/30/11331014/microsoft-windows-linux-ubuntu-bash
[10] https://www.theverge.com/2018/10/26/17954714/microsoft-github-deal-acquisition-complete
[11] https://www.theverge.com/2019/5/6/18534687/microsoft-windows-10-linux-kernel-feature
[12] https://www.theverge.com/2019/5/6/18527550/microsoft-chromium-edge-google-history-collaboration
[13] https://www.theverge.com/2019/9/6/20852451/microsoft-windows-10-powertoys-download-features
[14] https://techcommunity.microsoft.com/t5/microsoft-365-blog/microsoft-ignite-blog-microsoft-fluid-framework-preview/ba-p/978268

1.) Datensicherheit – Sicherstellung, dass Daten nicht manipuliert, geändert oder sonst wie kompromittiert werden können – und das über Gerätegrenzen und Dienstleistergrenzen hinweg
2.) Datensouveränität – Sicherstellung, dass der Endbenutzer entscheidet, wann darf welcher Dienst, welche Daten, zu welchem Zweck wie verarbeiten

Punkt 1 – Datensicherheit – lässt sich technisch schon lange lösen, im Open Source Bereich zum Beispiel durch den Einsatz von PGP[15] (starker Verschlüsselung) und GIT[16] in Kombination. Microsoft stellt dies in seiner Cloud als AIP – Azure Information Protection[17] zur Verfügung. Google und Amazon haben hier auch ihre entsprechenden technischen Lösungen, basierend auf demselben Prinzip.

Punkt 2 – Datensouveränität ist in Wahrheit die weitaus größere Herausforderung. Damit man versteht, was hier wann zum Einsatz kommt, muss man auch wieder die Vergangenheit in Erinnerung rufen und erklären, was da eigentlich passiert:

SAML
SAML war der erste Schritt um eine systemübergreifende Anmeldung (Single Sign On) implementieren zu können. Man hat eine Datenbank mit Benutzernamen und Passwort (oder Passworthash) und hinterlegt für jeden weiteren SAML Dienst die entsprechenden Accounts. Also eine zentrale Datenbank in der persönlichen Überwachung der hauseigenen IT, die mit anderen IT-Dienstleistern durch Zertifikatsaustausch föderieren – also einander vertrauen[18].
Je größer die Datenbank, je mehr Föderationen, desto interessanter für Hacker, Innenministerien und Nachrichtendienste[19],[20]

OAuth bzw. OAuth2
Egal ob Facebook, Microsoft, Apple oder Google man kann annehmen, dass diese durch die staatliche Zusammenarbeit in Demokratien genauso wie in Diktaturen, diesen eklatanten Architektur-Fehler, Benutzernamen mit Passwordhashes in einer gewaltigen Datenbank für möglichst viele Services zu speichern, erkannt haben. Auf Basis dessen, wurde das Konzept radikal umgestellt. Wenn Sie sich heute bei Microsoft oder Google anmelden, dann müssen sie sich zuerst identifizieren (ihre E-Mail-Adresse eingeben) und basierend auf ihrer Organisation (also alles nach dem @) werden sie weitergeleitet auf den Anmeldeserver ihrer Organisation. Dort können Sie sich entweder mit einem Passwort oder einem digitalen Zertifikat ausweisen und erhalten bei entsprechender Prüfung Zugang. Der Zugang ist ein Token, der für eine definierte Zeit gilt und der bestätigt, dass Sie tatsächlich Sie sind. Diesen Token können Sie gegen jeden anderen OAuth2 Dienst ebenso vorweisen und sämtliche Daten, die Sie mit anderen Diensten austauschen, werden basierend auf diesen Token und weiterer kryptografischer Verfahren stets digital verschlüsselt. Gleichzeitig muss jede fremde Organisation offenlegen, welche Daten Sie von Ihnen abfragt, auf welche Sie zugreifen möchte. End-to-End Encryption und der erste Schritt zu Datensouveränität.

---

[15] https://de.wikipedia.org/wiki/OpenPGP
[16] https://de.wikipedia.org/wiki/Git
[17] https://azure.microsoft.com/de-de/services/information-protection/
[18] https://www.shibboleth.net/
[19] https://www.heise.de/ct/artikel/Warum-ein-neues-GroKo-Gesetz-die-Meinungsfreiheit-einschraenken-wird-4798347.html
[20] https://www.heise.de/news/EU-Ratspraesidentschaft-Seehofer-treibt-die-Ueberwachungsunion-voran-4802114.html

Da wir allerdings unseren Benutzern beigebracht haben, sich mit der ganzen E-Mail-Adresse anzumelden, anstatt zuerst bekannt zu geben, bei welcher Organisation sie sind, gibt es hier noch Bedarf zur Weiterentwicklung/Umstellung, die technisch eigentlich schon gelöst ist.[21]

FIDO2
Echte Datensouveränität kann allerdings erst hergestellt werden, wenn der aus OAuth2 generierte Token nicht mehr Stunden oder gar Minuten Zugriff gewährt und auch der Benutzer selbst, jederzeit festlegen kann (und nicht nur bei der ersten Anmeldung bei einem fremden Dienst), wann, welcher Dienst, wofür Zugriff erhält. Dafür wurde das Konzept der passwortlosen Anmeldung entwickelt und deshalb unterstützt seit Februar 2020 jedes Betriebssystem diesen Standard. [22],[23],[24]

Warum kann es sich Microsoft leisten komplett Open Source zu gehen?

1.) durch die radikale Lizenzumstellung, die seit diesem Frühjahr global erfolgt. Microsoft 365 - eine Lizenz, die Cloud, Geräte und Office abdeckt – hinterfragen Sie, wo denn da genau die Kosten entstehen – beim Betrieb und Ausbau der Rechenzentren und der Infrastruktur oder bei der Entwicklung ohnehin offener Standards?[25]
2.) durch die radikale Öffnung sämtlicher Bildungs- und Schulungsunterlagen, die kostenlos global zur Verfügung stehen[26]
3.) durch die Zusammenarbeit und Offenlegung in der Forschung und Entwicklung[27]
4.) durch die aktive Kommunikation der Produktentwickler mit den Endkunden durch UserVoice[28]

Wie geht es weiter?

Da nun ohnehin auf Windows 10 ein voll funktionsfähiges Linux Subsystem vorhanden ist, ist der nächste Schritt eigentlich schon vorgezeichnet: Open Source Windows Subsystem.
Der Linux Kernel als der zentrale Kernel, die UI weiterentwickelt basierend auf Windows 10 – natürlich ebenso Open Source. Natürlich ist dies ein Prozess, der nicht von heute auf morgen erfolgen wird – es braucht Sicherheit und Kontinuität für die bestehenden Systeme der Kunden – aber dieser Tag rückt Stück für Stück näher.

Wer an die hämischen Stimmen, rund um die Einstellung von Windows Mobile denkt und wie das mit „mobile first – cloud first“ zusammenpasst, dem sollte nun das große Ganze wie Schuppen von den Augen fallen: Microsoft 100% Open Source (zumindest bald).

---

[21] https://www.heise.de/news/EU-Datenschuetzer-warnt-vor-unueberlegtem-Einsatz-von-Microsoft-Produkten-4836018.html
[22] https://www.heise.de/news/Passwortloses-Anmelden-Apple-bringt-Face-ID-und-Touch-ID-ins-Web-4795505.html
[23] https://www.heise.de/news/Neue-Website-der-FIDO-Allianz-erklaert-Einsteigern-die-passwortlose-Anmeldung-4768854.html
[24] https://www.heise.de/tests/Goldengate-Security-Keys-FIDO2-Sticks-mit-Fingerabdruckscanner-4717188.html
[25] https://www.microsoft.com/de-at/microsoft-365/business/compare-all-microsoft-365-business-products?&activetab=tab:primaryr2
[26] https://education.microsoft.com
[27] https://www.microsoft.com/en-us/research/
[28] Am Beispiel von Teams: https://microsoftteams.uservoice.com/

Wie können die Strafverfolgungsbehörden in Zukunft trotz 100% Verschlüsselung der Daten ihren Aufgaben nachkommen, so gibt es auch hier sinnvolle Ansätze, die es gilt, weiter zu Verfolgen.[29],[30]

Gastkommentar von Thomas Baldauf, IT-Manager am GRG 21 Ödenburger Straße, MIE Fellow

[29] https://www.heise.de/news/Bundesrat-stimmt-fuer-erweiterte-Pflicht-zur-Passwortherausgabe-4835693.html

[30]