

Interfraktionelle Interpellation AL/GaP/PdA, SP/JUSO (Simone Machado, GaP/Halua Pinto de Magalhães, SP): Nachkredit Schulinformatik base4kids2 - Fragen zu den strategischen und datenschutzrelevanten Folgen

Immer wieder wird von Technik- und Wirtschaftsexperten auf die Gefahren hingewiesen, die ein sog. "Vendor Lock -In"¹ für die Betroffenen mit sich bringt. Die Abhängigkeit vieler Stellen der Öffentlichen Hand von einem einzigen Software-Anbieter (Microsoft) ist bereits heute enorm. Um Kund*innen zu gewinnen, locken Anbieter wie Microsoft zumeist mit attraktiven Startangeboten. Die Folgekosten werden jedoch bei Kaufentscheidungen selten mitkalkuliert. Langfristig profitieren daher die Hersteller von der Bindung mehr als die Kund*innen. Der Hersteller kann die Preisschraube jederzeit andrehen. Diese Lock-in-Bindungen gibt es im Informationszeitalter bei Hardware- und Software-Produkten. Der Lock-In in Schulen wird deutlich stärker ausfallen und gefährdet die digitale Souveränität. Produktschulungen verhindern digitale Mündigkeit. Ein selbstbestimmtes Handeln ist, selbst bei vorhandenem politischen Willen - wie auch das base4kids2 Projekt anschaulich zeigt - mit teilweise unwägbareren Risiken verbunden. Und mit jedem neuen Projekt, das wieder Software vom selben Hersteller beschafft, wächst diese Abhängigkeit, steigen die Risiken.

Die Entscheidung, bei der Software für base4kids2 explizit auf eine eigene - d.h. selbst in Auftrag gegebene - Lösung auf Basis von Open Source zu setzen, war also ursprünglich richtig. Jedoch sind sowohl in der Organisation, Projektdurchführung als auch in der technischen Planung und Umsetzung offensichtlich Fehler passiert, die zu einem unbefriedigenden Ergebnis geführt haben. Diese Fehler dürfen nun nicht zum Anlass genommen werden, die Bemühungen, um eine Verringerung des Lock-In-Effekts für die Stadt Bern zu schwächen oder gar einzustellen. Vielmehr sollten sie als Lehren für zukünftige Projekte dienen, damit die Souveränität in Informatikvorhaben wieder verstärkt und die einseitige Abhängigkeit reduziert werden kann.

Mit der Umstellung auf internetbasierten Lösungen kommen nun auch fundamentale Fragen des Datenschutzes auf. Sowohl Office365 als auch Teams sind cloud-basierte Software-Pakete. D.h. es werden neben Kommunikationsdaten und Dokumenten sowohl personenbezogene als auch Verhaltensdaten an die Cloud-Betreiber übertragen. Darüber hinaus werden Telemetriedaten über verschiedene Nutzungsparameter, Netzwerk usw. erhoben. Eine Auswertung dieser Daten erlaubt das Erstellen umfangreicher und verschiedenartiger Profile sowohl der Schüler*innen als auch der Lehrpersonen.

Besonders bei Schüler*innen ist dies als kritisch einzustufen. Sie werden hier ohne eigenes Zutun und ohne die Möglichkeit zu Gegenmassnahmen einer global vernetzten Werbe- und Unterhaltungsindustrie als Neukunden zugeführt. Ihre Daten werden zentral (und wohl ausserhalb der Schweiz, evtl. sogar Europas) gespeichert und verarbeitet. Über die Art der Verarbeitung sowie Dauer der Speicherung geben die MS-Nutzungsbedingungen wenig konkrete Auskünfte. Darüber hinaus ist z.B. die Nutzung der Microsoft-eigenen Suchmaschine Bing und der Software-Plattform GitHub explizit von den Datenschutzbestimmungen ausgenommen. D.h. werden diese Dienste

¹ Der Begriff des Lock-In-Effekts stammt aus der Betriebswirtschaft und den Wirtschaftswissenschaften. Ein Lock-In bindet Kund/innen an ein bestimmtes Produkt, weil sich ein Wechsel zu einem Konkurrenzprodukt wirtschaftlich nicht lohnt. Erreicht wird dies durch fehlende Interoperabilität zwischen den Produkten.

<https://www.heise.de/hintergrund/Schule-digital-Wie-der-Lock-In-Effekt-unsere-Schulen-beschaenkt-6006927.html>

durch die Schüler*innen verwendet, unterliegen die so erhobenen Daten anderen, d.h. deutlich schwächeren, Schutzbestimmungen.

Auch hier war der ursprünglich gewählte Weg mit einer schweizerischen Anbieterin und Datenspeicherung nur auf dedizierten Servern in der Schweiz wohl der richtige. Auch, da hier eine viel weitergehende Einflussnahme auf die Datenschutzbestimmungen möglich war, als dies etwa bei der Nutzung von MS-Diensten der Fall sein wird. Mit dem nun geplanten Umstieg auf die angesprochenen MS-Produkte gibt man markante Vorteile hinsichtlich des Datenschutzes und Souveränität grösstenteils auf. Die so erhoffte (im Übrigen auch noch nicht erwiesene) Verbesserung der Benutzbarkeit der Plattform base4kids2 kommt also mit einem Preis, der sich nicht nur an der Höhe des beantragten Nachtragskredits bemisst und ist durchaus risikoträchtig.

Wir ersuchen den Gemeinderat höflich um die Beantwortung der nachfolgenden Fragen.

1. Mit dem geplanten Wechsel auf Microsoft (MS)-Produkte für die base4kids2-Plattform schafft man sich neue Probleme in Bezug auf Datenschutz und Lieferanten-Abhängigkeit. Dies, obwohl der Wille zur Reduktion dieser Abhängigkeit unbestritten ist (z.B. 2013.SR.000095) und in Strategien festgehalten wird:
 - a. Welche Massnahmen werden getroffen, um die persönlichen Daten der Schüler*innen angemessen zu schützen ("Microsoft-Login", "Apple-ID")?
 - b. Welche Massnahmen werden getroffen, um den grösser statt kleiner werdenden Gefahren aus dem drohenden Vendor-Lock-in zu begegnen?
 - c. Wie beurteilt der Gemeinderat die Tatsache, dass sowohl EU-Datenschützer als auch die deutsche Datenschutzkonferenz den Einsatz dieser MS-Produkte an Schulen aus Sicht des Datenschutzes als heikel² erachten?
2. Die Beschaffung von Informatiklösungen auf der Basis von Open-Source-Produkten ist nicht 1:1 identisch mit derjenigen von proprietärer Software. Sie stellt andere Anforderungen u.a. an Projektmanagement, Ausschreibung und Controlling, um erfolgreich zu sein.
 - a. Welche Massnahmen (hinsichtlich Weiterbildung, Personalressourcen etc.) werden getroffen, damit zukünftige IT-Projekte auf Open-Source-Basis erfolgreich durchgeführt werden können?
 - b. Hat der Gemeinderat die Folgekosten der Bindung an die Microsoft-Standardlösung miteinberechnet und von welchen Kosten geht er aus?
 - c. Wie stellt der Gemeinderat die digitale Mündigkeit sicher, d.h. dass Lehrpersonen und Schüler*innen, die in Zukunft auf ihren privaten Geräten Open-Source-Lösungen benützen wollen, dies auch tun können?

²<https://www.heise.de/news/Datenschuetzer-sehen-Microsoft-365-in-Behoerden-als-nicht-rechtskonform-an-4893604.htm>

Bern, 20. Mai 2021

Erstunterzeichnende: Simone Machado, Halua Pinto de Magalhães

Mitunterzeichnende: Jemima Fischer, Eva Gammenthaler, Timur Akçasayar, Daniel Rauch, Katharina Altas, Lena Allenspach, Laura Binz, Diego Bigger, Ayse Turgul, Valentina Achermann, Mohamed Abdirahim, Fuat Köçer, Tabea Rai, Bettina Stüssi, Sara Schmid, Bernadette Häfliger, Ingrid Kissling-Näf, Michael Sutter, Nora Krummen, Barbara Nyffeler, Alina Irene Murano, Zora Schneider