Die FRAKTION
im Rat der Stadt Troisdorf

Die FRAKTION – UWG Regenbogen und Die PARTEI
Kölner Str. 176, 53840 Troisdorf
kontakt@die-fraktion-troisdorf.de

An:

Bürgermeister Alexander Biber

Troisdorf, 1.04.2021

Antrag: OpenSource Software in der Stadtverwaltung

Sehr geehrte Herr Bürgermeister,

hiermit beantragt Die FRAKTION über folgenden Beschlussentwurf in der nächsten Sitzung des Ausschusses für Bürger*Innenbeteiligung, Digitalisierung, Beteiligungssteuerung und Verbraucherschutz abzustimmen.

Die Verwaltung der Stadt Troisdorf wird angehalten wo immer möglich Open-Source-Software einzusetzen. Wo dies nicht möglich ist, ist auf von der Verwaltung entwickelte oder zur Entwicklung beauftrage Software zu setzen, welche der Allgemeinheit zur Verfügung zu stellen ist.

Begründung

In der Vergangenheit kam es zu größeren Vorfällen in der IT-Sicherheit aufgrund von Sicherheitslücken in proprietärer Software. Als jüngstes Beispiel sei hier der Microsoft Exchange Server genannt, welcher am 3. März 2021 durch Microsoft ein kritisches Update erhalten hat. Das Bundesamt für Sicherheit in der Informationstechnik hat in seiner Pressemitteilung vom 5. März 2021 die Anzahl der Betroffenen im Bundesgebiet auf mehr als 9.000 Betreiber geschätzt und die IT-Bedrohungslage hinsichtlich dieser Schwachstelle als Rot kategorisiert. Der sog. CVSS-Score, welcher die Kritikalität einer Sicherheitslücke anzeigt, lag bei 9,1 von 10 und erforderte weltweit ein sofortiges Einspielen von Updates (vgl. BSI-Meldung https://t1p.de/1lxt).

Gründe für solche kritischen Schwachstellen sind unter anderem, dass der Code dieser Software nur von den Entwicklern bzw. den internen Fachleuten auf Sicherheitslücken geprüft wird. Auch Geheimdienste wie die National Security Agency in den Vereinigten Staaten von Amerika hat in der Vergangenheit vermehrt Sicherheitslücken in Software-Produkten gefunden und verheimlicht (vgl. EternalBlue – CVE 2017-0144, Bericht in der NY-Times: https://t1p.de/8tqo). Sobald solche Lücken von Cyberkriminellen gefunden werden, ist der Schaden immens hoch und kann Unternehmen und auch öffentliche Stellen an einer Weiterarbeit hindern. Als Beispiel für die EternalBlue-Lücke sei hier die WannaCry-Ransomware angeführt (Artikel von Heise-Online: https://t1p.de/6gxq), welche Krankenhäuser lahmlegte und auch die Deutsche Bahn zum Teil infizierte. Als Beispiel für weitere Sicherheitslücken sei der Angriff auf die Stadtverwaltung Angermünde vom 30. März 2021 genannt, welcher die Verwaltung bis voraussichtlich dem 7. April lahmlegt (Artikel vom Nordkurier: https://t1p.de/sn2g).

Bei Open-Source-Software wird der Quellcode grundsätzlich veröffentlicht. Dies schafft sowohl bei Bürger*Innen sowohl als auch bei Interessensverbänden wie dem Chaos Computer Club Vertrauen in das eingesetzte Software-Produkt (vgl. Corona-WarnApp) und verringert so die Angriffsvektoren für Cyberkriminelle erheblich. Ebenfalls ist die Nutzung und Verbreitung von Open-Source-Software kostenfrei und erfordert keine jährlichen Lizenzabgaben. Etwaige Fehler im Code können aufgrund der Tatsache, dass die Software und deren Quellcode öffentlich ist, schneller gefunden und von jedem Menschen weltweit behoben werden. Dadurch steigt auch der Qualitätsdruck der Entwickler und die Software wird erstaunlich gut dokumentiert. Diese Vorteile sind auch der Stadt Dortmund aufgefallen. Aus diesem Grunde hat der Rat der Stadt Dortmund am 11. Februar 2021 einen ähnlichen Beschluss gefasst und unterstützt somit aktiv die Open-Source-Community.

Als Nachteil sei jedoch der unter Umständen fehlende Herstellersupport im Fehler- und Problemfall erwähnt, besonders bei der Adaptierung von bereits bestehender Open-Source-Software. Hierbei existiert jedoch meist eine aktive Community, welche bei Problemen aktiv unterstützen kann. Auch wenn Fehler schneller gefunden werden können, können natürlich auch schneller Schwachstellen gefunden werden. Viele Experten auf diesem Gebiet arbeiten jedoch im Rahmen des sog. Bug-Bounty-Programms, welche Schwachstellen zunächst an den Entwickler melden, damit dieser die Schwachstelle beheben kann.

In der letzten Zeit veröffentlichen viele Unternehmen, unter anderem auch Microsoft, Apple und die SAP, Quellcodes von Software. Hier sei als Beispiel die Microsoft PowerShell oder die Corona-WarnApp des Bundesgesundheitsministeriums in Zusammenarbeit mit IBM und der SAP angeführt. Insbesondere letztere hat durch die Veröffentlichung des Quellcodes einen enormen Vertrauensvorsprung erhalten. Funktionen der proprietären App „Luca“, welche zum Zeitpunkt der Verfassung dieses Antrages keinen offenen Quellcode besitzt, werden nun laut Angaben des Bundesgesundheitsministeriums in die Corona-WarnApp adaptiert um diese sinnvolle Funktion zu nutzen, jedoch nicht von einem geschlossenen Quellcode und damit etwaigen Schwachstellen bei diesen höchst sensiblen Daten abhängig zu sein (Artikel der Tagesschau: https://t1p.de/9j5z). Die Entwicklung dieser Funktion kann von Experten und Fachleuten dank des offenen Quellcodes nachvollzogen werden und verbessert so auch die Transparenz der Behörden und Ministerien, was unsere Fraktion sehr begrüßt.

Mit freundlichen Grüßen,

Kai Huneke, Stadtverordneter Justin Fingerhuth, SKB Falko Hupp, SKB