sipgate

sipgate GmbH – Gladbacher Str. 74 – 40219 Düsseldorf

Bundesministerium des Innern, für Bau
und Heimat
Referat CI1
Grundsatz; Cyber- und
Informationssicherheit

Per E-Mail an: CI1@bmi.bund.de

Düsseldorf, den 8.12.2020

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Sehr geehrte Damen und Herren,

zunächst möchten wir uns für die Gelegenheit zur Stellungnahme bedanken. Eine umfassende Würdigung war in der Kürze der Zeit nicht möglich. Wir konzentrieren uns daher im Folgenden auf die die Telekommunikationsbranche betreffenden Änderungen.

Die sipgate GmbH ist ein mittelständisches Telekommunikationsunternehmen mit etwa 500.000 aktiven Telekommunikationsanschlüssen im Festnetz- und Mobilfunkbereich und beschäftigt knapp 200 Mitarbeiter. Der Schwerpunkt des Angebotes liegt in innovativen IT-gestützten Telekommunikationslösungen, in denen die Grenzen zwischen Festnetz und Mobilfunk aufgelöst werden. Die sipgate betreibt über Schwesterunternehmen ein eigenes Festnetz und zwei virtuelle Mobilfunknetze (davon eines als so genannter full MVNO (virtueller Mobilfunknetzbetreiber) im Netz der Telefonica Deutschland).

Die durch den Gesetzentwurf drohenden Belastungen durch zum Teil sehr fragwürdige und zum Teil noch gar nicht klar umrissene Auflagen bedrohen die Existenz des Unternehmens als innovatives und flexibles softwarebasiertes Telekommunikationsunternehmen. Einen relevanten Teil der Zertifizierung würde nach den bisher kommunizierten Vorstellungen der BNetzA und des BSI nämlich ein so genannter Code-Audit darstellen, bei dem unabhängige Dritte damit beauftragt werden den Quellcode der IT-Anwendungen darauf zu kontrollieren, ob unerwünschte Funktionen eingeschleust und versteckt wurden. Die schiere Menge des bereits heute bei der sipgate vorhandenen Computercodes macht eine Prüfung wirtschaftlich unmöglich und führt direkt zu einem Bankrott des Unternehmens.

Hinzu kommt, dass eine Zertifizierung im Falle der sipgate auch nicht das augenscheinliche Ziel erreicht. In aller Regel kaufen Telekommunikationsdiensteanbieter und -Netzbetreiber Ihre Ausrüstung bei Dritten (wie beispielsweise der Fa. Huawei) und nutzen diese dann zum Angebot von Diensten. Sipgate als Innovator im Markt hingegen entwickelt selbständig Software für Telekommunikationsdienste und -Netze, um sich vom Wettbewerb durch individuelle Dienstmerkmale abzugrenzen. Durch dieses Vorgehen sind Sabotage und Spionage durch Dritte schon deshalb ausgeschlossen, weil in der Wertschöpfungskette der sipgate keine Dritten existieren. Eine Verpflichtung zur Zertifizierung würde daher keinen Mehrwert an Sicherheit mit sich bringen.

Vorab möchten wir darauf hinweisen, dass der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG bereits Anfang des Jahres komplett überarbeitet und zum Teil erheblich verschärft wurde. Der damit verbundene Aufwand für die betroffenen Unternehmen war beträchtlich. Es ist nicht ersichtlich warum die entsprechenden Auflagen nun nochmals überarbeitet und verschärft werden, zumal in diesem Zusammenhang und damit erst vor wenigen Monaten eine intensive Abstimmung der betroffenen Bundesämter und der Unternehmen erfolgt ist.

1. Zertifizierungspflichtige Unternehmen

In der Sache wird durch den Entwurf nunmehr - entgegen der Regelungen des Kataloges von Sicherheitsanforderungen nach 109 TKG eine Zertifizierungspflicht für kritische Komponenten auch für mittelständische Unternehmen eingeführt. Die Regelungen im § 109 TKG führen nach diesseitigem Verständnis dazu, dass der Katalog der kritischen Komponenten iSd § 109 Absatz 6 des TKG (neu) allein maßgeblich wird. Dieser ist - anders als die kritischen Komponenten für andere Bereiche, welche gesetzlich festgelegt werden sollen - in einem relativ einfachen Verwaltungsverfahren änderbar. Dadurch entstehen Unsicherheiten hinsichtlich der konkret zu

sipgate

zertifizierenden Netzkomponenten. Warum hier für die Telekommunikationsbranche ein Sonderweg gewählt wird ist nicht verständlich.

In dem Katalog der Sicherheitsanforderungen der BNetzA iSd § 109 TKG (alt) war eine Einschränkung des Kreises der Verpflichteten (“Betreiber mit erhöhtem Gefährdungspotential”) auf 5G-Mobilfunknetzbetreiber mit Frequenzzuteilungen vorgenommen worden. Nach der Logik des aktuellen Kataloges, dem auch der Entwurf zu folgen scheint, soll eine Zertifizierung also nur Betreiber mit erhöhtem Gefährdungspotential betreffen, soweit diese kritische Komponenten laut Liste der kritischen Komponenten betreiben.

Der § 109 Abs. 2 S. 3 TKG neu hebelt diese Einschränkung nunmehr aus und belastet auch alle anderen Nutzer von kritischen Komponenten generell. Die die Unternehmen belastenden Regelungen sollten aber unter Berücksichtigung der Gefährdungslage sowie der durch Angriffe verursachten potentiellen Schäden abgestufte Auflagen formulieren, die mit zunehmender Gefahr bzw. mit zunehmendem Schaden für die Allgemeinheit, höhere Auflagen regeln. Hierbei ist zu berücksichtigen, dass die Gefahrenlage für ein kleineres Unternehmen eine andere (nämlich weniger konkret und wahrscheinlich) ist als für große Unternehmen, da diese als Ziel eines Angriffes weniger attraktiv sind. Auch die Auswirkungen für die Allgemeinheit bzw. die öffentliche Sicherheit wären weitaus weniger spürbar als bei einem erfolgreichen Angriff auf ein großes Unternehmen.

Die Änderungen des § 109 ergänzen sich jedoch nicht in diesem Sinne, die überlappende Wirkung der Regelung für die kritischen Komponenten widerspricht sogar dem Ziel nur Betreiber mit erhöhtem Gefährdungspotential zu erfassen. Der Eingriff ist somit auch nicht verhältnismäßig und angemessen. Da dem Einvernehmen von BMWi, BNetza und BSI nach der Kreis der zur Zertifizierung Verpflichteten auf Betreiber öffentlicher Telekommunikationsnetze des Mobilfunks der 5. Generation mit Frequenzzuteilungen beschränkt bleiben sollte, muss die Regelung in der Novelle des TKG entsprechend angepasst werden und darf nur Anbieter mit erhöhtem Gefährdungspotenzial betreffen. Die generelle Zertifizierungspflicht für kritische Komponenten - auch in Netzen von Unternehmen kleiner oder mittlerer Größe - stellt einen unverhältnismäßigen und zu pauschalen Eingriff dar.

Zudem ist das ursprüngliche Ziel der Regelungen, die Gefährdung durch ausländische Dienste oder andere Akteure zu minimieren, komplett aus dem Fokus geraten. Im Gegenteil gibt nun der Gesetzgeber in seiner Begründung sogar explizit an, dass eine Zertifizierung von Software keine geeignete Maßnahme darstellt, um Sabotage und Spionage zu verhindern. Dennoch wird an den avisierten Maßnahmen festgehalten, ohne dass ein Ziel der Maßnahmen ersichtlich wäre.

sipgate GmbH
Gladbacher Str. 74
40219 Düsseldorf

Telefon 0211 – 63 55 55 - 0
Telefax 0211 – 63 55 55 - 22
info@sipgate.de

Geschäftsführer:
Tim Mois
Thilo Salmon

Konto 181 14 88 00
BLZ 300 400 00
Commerzbank

Steuernr. 10657247147
HRB 39841, Düsseldorf
U.-St.-ID DE219349391

sipgate

2. Inhalt und Gegenstand der Zertifizierung

Da die konkrete Art und Weise der Zertifizierung nach wie vor komplett unklar ist, sind wir gezwungen hier den Rahmen für etwas zu diskutieren, dessen Inhalt wir nicht kennen. Das macht eine Kommentierung des Gesetzes schwierig bis unmöglich.

Nach diesseitiger Auffassung ist eine sinnvolle Zertifizierung von Free-and-Open-Source-Software (FOSS), selbst entwickelter Software bzw. von in kurzen Zyklen entwickelter oder gepatchter Software mit angemessenen Mitteln nicht möglich.

Soweit Telekommunikationskomponenten am Markt für eine Vielzahl von Kunden entwickelt und angeboten werden, ist eine Prüfung und Zertifizierung in wirtschaftlicher Hinsicht evtl. noch denkbar, da sich der Aufwand auf diverse Abnehmer verteilt. Bei Eigenentwicklungen oder FOSS ist dies jedoch nicht der Fall.

In den letztgenannten Fällen ist eine Zertifizierung jedoch auch nicht erforderlich.

An dieser Stelle möchten wir kurz den Umgang der sipgate mit dem Thema IT-Sicherheit darstellen, um zu verdeutlichen, dass eine Zertifizierung weder wirtschaftlich noch inhaltlich möglich ist.

Sicherheit als Ziel ist in unseren Unternehmen tief verankert. Daher haben wir bereits in der Vergangenheit ein Sicherheitskultur geschaffen, die diesem Ziel Rechnung trägt.

Software bei sipgate wird generell nach dem 4-Augen-Prinzip entwickelt. Dabei teilen sich regelmäßig wechselnde Paarungen zweier Entwickler jeweils eine Aufgabe. Jede geschriebene Zeile Code wird dabei von mindestens zwei Entwicklern gelesen, verstanden und zur weiteren Prüfung in die Testumgebungen eingepflegt. Schon durch dieses Prinzip wird die Zahl der potentiellen Sicherheitslücken minimiert.

Von dort aus wird der neu geschriebene bzw. redigierte Code nach dem Durchlaufen weiterer Tests in die Produktivumgebung übergeben. Es sei hervorgehoben, dass hierbei etwaige Abhängigkeiten mitigiert werden und sipgate gemäss dem Prinzip von “Continuous Delivery” Neuigkeiten direkt den Endkunden verfügbar macht.

Ferner arbeitet sipgate mit einer so genannten “Zero-Bug-Policy”. Dieses Prinzip gibt vor, dass bekannte Softwaremängel, unabhängig davon, ob es sich um funktionale oder Sicherheitsmängel handelt, vorrangig zu beheben sind.

sipgate GmbH
Gladbacher Str. 74
40219 Düsseldorf

Telefon 0211 – 63 55 55 - 0
Telefax 0211 – 63 55 55 - 22
info@sipgate.de

Geschäftsführer:
Tim Mois
Thilo Salmon

Konto 181 14 88 00
BLZ 300 400 00
Commerzbank

Steuernr. 10657247147
HRB 39841, Düsseldorf
U.-St.-ID DE219349391

Diese Prinzipien, also sowohl das “Pair Programming” genannte 4-Augen-Prinzip, als auch “Continous Delivery” entsprechen dem aktuellen Stand der Technik in der Softwareentwicklung. Eine moderne Softwareentwicklung ohne diese beiden Prinzipien ist kaum vorstellbar, da andernfalls zahlreichen Fehlerquellen und Unsicherheiten Vorschub geleistet würde und die Softwareentwicklung in größeren Intervallen ein hohes Risiko an Fehlentwicklungen begründet. Ebenso sind es diese Prinzipien, denen sipgate die Möglichkeit verdankt, als kleiner Anbieter an einem Markt teilzunehmen, der von Großunternehmen geprägt ist.

Eine Zertifizierung, die in Zyklen erfolgt, ist fundamental inkompatibel mit dem Entwicklungsmodell “Continuous Delivery”, dass der sipgate GmbH ihre Marktposition sichert, und bedroht daher das Unternehmen in seinen Grundfesten.

Die sipgate GmbH befürchtet, durch eine verbindliche Zertifizierung vor eine unlösbare Aufgabe gestellt zu werden. Allein die Codebasis der elementaren, zentralen Systeme hat eine Größe von 1,5 Million Zeilen Quellcode. Hinzu kommen die Codes für die eingesetzten Werkzeuge, wie Compiler und Code-Management-Tools, externe Bibliotheken und die Quellcodes des unterliegenden Betriebssystems - alles in allem auf jeden Fall mehr als 10 Millionen Zeilen Quellcode.

Selbst unter der positiven Annahme, ein Zeile-für-Zeile-Audit könnte durch geeignet einschränkende Thread Models eine Geschwindigkeit von 500 Zeilen pro Stunde erreichen, wären netto mehr als 20.000h Stunden an Analyse zu bewältigen - zu Kosten die das Jahresergebnis der sipgate GmbH bei weitem überschreiten.

Dabei würde die direkte finanzielle Belastung nur einen Teil der Belastung darstellen. Sipgate hat sich derart im Markt positioniert, dass ein kontinuierlicher Ausstoß an Innovationen produziert wird. Diese Arbeitsweise ist Stand der Technik in der Internet-Branche, aber nicht in der TK-Branche. Letztere ist von großen Marktteilnehmern und langen Innovationszyklen geprägt, die Ihre Systeme von externen Herstellern beziehen, während die erfolgreichen Player in Internetmärkten allesamt Ihre Software-Systeme zu entscheidenden Teilen selbst gestalten und entwickeln, um kontinuierlich Innovationen zu produzieren. Genau dieser Innovationsvorteil erlaubt es sipgate als kleinem Teilnehmer in einem Markt gegen große Wettbewerber zu bestehen.

2.1. Keine externe Zertifizierung von Eigenentwicklungen

Beim Bemühen, externe und insbesondere staatliche Eingriffe in die Software und Netze von Telekommunikationsanbietern wirksam zu begegnen, darf nicht vergessen werden, dass europäische Anbieter, die Ihre Software selbst entwickeln, jedenfalls bisher keinem substantiellen staatlichen Einfluss ausgesetzt sind. Ein solcher Anbieter “kennt” und versteht seine Infrastruktur

sipgate

und weiss um die Authentizität seiner Systeme. Dies gilt insbesondere für Anbieter der Softwareentwicklungsbranche, die durchgängig nach dem 4-Augen-Prinzip Software entwickeln und sich auf diese Weise auch vor Angriffen durch Insider schützen.

Ein Eingriff in dieses gesunde Entwicklungsumfeld würde die betroffenen Unternehmen belasten, ohne einen Mehrwert in Form von gewonnener Sicherheit zu schaffen - zum Schaden von Wettbewerb und Innovation. Zum Schutz vor einer Abhängigkeit von Nicht-EU-Herstellern gilt es daher die Entwicklung von TK-Systemen in Deutschland im Mittelstand zu fördern und nicht etwa, wenngleich gut gemeint, zur be- oder verhindern.

Im Ergebnis würde eine Zertifizierung dieser eigenentwickelten Komponenten auch keinen Mehrwert bringen, da der Anbieter ja ohnehin jederzeit in kritischer Weise in seine Systeme eingreifen kann und diese im Extremfall abschalten könnte.

2.2. Keine externe Zertifizierung von FOSS

Free-and-Open-Source-Software (FOSS) gilt gemeinhin als Innovationstreiber - auch für Internet- und Telekommunikationsunternehmen. Die Grundfeste des Internet wurden auf Basis von FOSS-Systemen errichtet und in zahlreichen Märkten dominieren FOSS-Anwendungen. Es ist kein Zufall, dass gerade in Märkten, die maßgeblich von Innovation getrieben werden, zahlreiche FOSS-Anwendungen zu Einsatz kommen. So laufen nahezu 100% der 500 größten Computer der Welt unter Linux (FOSS Betriebssystem) und mehr als zwei Drittel aller Webserver unter FOSS[1]. Vergleichbares gilt für den Domain Name Service (DNS) und zahlreiche andere Kerndienste im Internet.

FOSS bietet den Vorteil, dass weltweit eine große Anzahl an verschiedenen Entwicklern und Entwicklerteams Systeme entwickeln, sich gegenseitig überprüfen und Sicherheitslücken aufdecken. Dadurch ergibt sich für den Einzelnen der Vorteil, dass er schneller an großen Entwicklungen partizipieren kann und Sicherheitslücken, wie sie in jeder Software bestehen können, zeitnah gefunden und geschlossen werden können. Es suchen also nicht nur die Angestellten eines einzelnen Unternehmens nach Sicherheitslücken, sondern eine weltweite Gemeinschaft. So werden Sicherheitslücken bei FOSS üblicherweise schneller aufgedeckt als bei proprietärer Software, wo persönliche, finanzielle und wirtschaftliche Interessen der beteiligten Personen und Unternehmen gegen eine Aufdeckung von Sicherheitslücken sprechen können und unternehmensinterne Abläufe oftmals für zeitliche Verzögerungen sorgen. Werden bei FOSS Sicherheitslücken aufgedeckt, ist es jedem Mitglied der FOSS-Gemeinschaft möglich, entsprechende Warnhinweise zu veröffentlichen und notwendige Änderungen anzustoßen. Im Vergleich dazu sind Entwicklungs-, Überprüfungs- und Verbesserungsverfahren bei proprietärer Software in aller Regel langwierig.

[1] https://en.wikipedia.org/wiki/Usage_share_of_operating_systems#Market_share_by_category

sipgate

Dabei ist die Vorgehensweise bei der Entwicklung jedoch fundamental inkompatibel mit einer Zertifizierung. In aller Regel existiert schlicht kein erkennbarer Hersteller, der gegenüber einer Zertifizierungsstelle die Verantwortung übernehmen könnte, da gerade die erfolgreichen Projekte von einer Vielzahl an Beteiligten getragen werden. Erfreulicherweise verfolgen jedoch die Zertifizierung als auch FOSS-Projekte das gleiche Ziel, nämlich den Schutz vor Fehlern, die zu einer Beeinträchtigung von Diensten führen. So ist es, anders als bei proprietären Systemen, einem Kommunikationsanbieter möglich, nachzuvollziehen, von welchem Beteiligten welche Änderung am Quelltext beigetragen wurde. Bösartige Änderungen werden daher in aller Regel kurzfristig erkannt und die Beteiligten von der weiteren Mitarbeit gesperrt. Ebenso ist es aufgrund des vorhandenen Quellcodes möglich, im Falle von Manipulationen im Nachgang leicht zu erkennen, wie es zu den Manipulationen kam. Nach alledem ist eine Zertifizierung für den Bereich Free-and-Open-Source-Software weder sinnvoll möglich aus Sicherheitsgründen noch erforderlich.

Eine Verpflichtung zur Zertifizierung von FOSS im Bereich der Telekommunikation würde zu einem nachhaltigen Verlust von Innovationskraft führen, den Wettbewerb zum Nachteil kleinerer Anbieter erheblich beeinflussen und die Innovation stark beeinträchtigen.

Nach alledem ist vor dem Hintergrund der gerade erst kürzlich erfolgten Verschärfung der Anforderungen für Telekommunikationsunternehmen sowie des nicht messbaren Mehrwerts einer Zertifizierung im Vergleich zu den innovativen Softwareentwicklungsmethoden eine weitere Verschärfung nicht gerechtfertigt und auch nicht erforderlich. Die Zertifizierungspflicht darf im Vergleich zu den Regelungen im Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) nicht erweitert werden.

Als sehr unglücklich empfinden wir die sehr kurz bemessene Frist zur Stellungnahme sowie die zeitliche Überschneidung mit den ebenfalls derzeit noch nicht final abgestimmten Änderungen durch die Novelle des Telekommunikationsgesetzes.

Mit freundlichen Grüßen

sipgate GmbH
Thilo Salmon
Geschäftsführer

sipgate GmbH
Gladbacher Str. 74
40219 Düsseldorf

Telefon 0211 – 63 55 55 - 0
Telefax 0211 – 63 55 55 - 22
info@sipgate.de

Geschäftsführer:
Tim Mois
Thilo Salmon

Konto 181 14 88 00
BLZ 300 400 00
Commerzbank

Steuernr. 10657247147
HRB 39841, Düsseldorf
U.-St.-ID DE219349391