Vertrauenswürdigkeit von Herstellern

Für den Einsatz eines zertifizierten Produktes in einem sensiblen Umfeld ist neben der Zertifizierung wesentlich, ob der jeweilige Hersteller des Produktes hinreichend vertrauenswürdig ist. Im Rahmen der Produktzertifizierung prüft das BSI nicht, ob der Hersteller diese Vertrauenswürdigkeit aufweist. Mit einer Zertifizierung ist daher keine Aussage zur Vertrauenswürdigkeit des Herstellers verbunden.

Sollte ein Bedarfsträger in einem öffentlichen Vergabeverfahren (als Behörde) oder im Rahmen einer privatwirtschaftlichen Ausschreibung (als Unternehmen) spezielle Anforderungen an die Vertrauenswürdigkeit eines Herstellers haben, können weitere Zuschlags- und/oder Eignungskriterien sowie Voraussetzungen zur Durchführung des Vertrages herangezogen werden. Insgesamt ist allerdings darauf zu achten, dass diese keinen Ersatz für eigene IT-Sicherheitsmaßnahmen darstellen.

Im Folgenden werden beispielhaft Punkte aufgeführt, auf die in den Kriterien und Voraussetzungen eingegangen werden kann . Die Details sind durch den Bedarfsträger für den jeweils zu vergebenen Auftrag im Rahmen einer Einzelfallprüfung festzulegen und zu begründen. Insbesondere muss jede Einschränkung des Wettbewerbs auf objektiven, d.h. unabhängig nachprüfbaren, erforderlichen und diskriminierungsfreien Kriterien beruhen (s. hierzu auch Erlass und Handreichung des Bundesministerium des Innern zur „No-Spy-Klausel“ http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/no-spy-erlass.html). Im Fall eines privatwirtschaftlichen Unternehmens als Bedarfsträger sind die Formulierungen sinngemäß anzupassen.

1. Der Hersteller verpflichtet sich, mit dem Bedarfsträger auf sicherheitstechnischem Gebiet intensiv zu kooperieren und insbesondere frühzeitig über neuartige Produkte, Technologien und Updates bestehender Produktlinien zu informieren.
2. Der Hersteller legt dem Bedarfsträger seine gesamtwirtschaftliche Situation offen. Dies umfasst beispielsweise die Beteiligungsverhältnisse am Unternehmen, sowie die Jahresabschlüsse der letzten Jahre.
3. Der Hersteller versichert, dass er keine Informationen aus seinen Vertragsverhältnissen mit der Bundesrepublik Deutschland oder einer ihrer Stellen an Dritte weitergibt.
4. Der Hersteller verpflichtet sich, durch organisatorische und rechtliche Maßnahmen sicher zu stellen, dass vertrauliche Informationen von oder über seine(n) deutsche(n)

staatliche(n) Kunden nicht auf eigene Veranlassung oder Veranlassung Dritter in das Ausland gelangen oder ausländischen Stellen im Inland zur Kenntnis gelangen.

5. Der Hersteller versichert, dass er rechtlich und tatsächlich in der Lage ist, keine vertrauliche Informationen von oder über deutsche(n) staatliche(n) Kunden an Dritte weiterzugeben. Insbesondere bestehen zum Zeitpunkt der Abgabe der Erklärung keine Verpflichtungen, Dritten solche Informationen zu offenbaren oder in anderer Weise zugänglich zu machen. Dies gilt nicht, soweit hierfür gesetzliche Offenlegungspflichten zu Strafverfolgungszwecken bestehen, es sei denn, solche Offenlegungspflichten bestehen gegenüber ausländischen Nachrichten- oder Sicherheitsbehörden. In Zweifelsfällen weist der Hersteller auf die gesetzliche(n) Offenlegungspflicht(en) vor Abgabe der Erklärung hin.
6. Der Hersteller verpflichtet sich, den Bedarfsträger sofort schriftlich zu benachrichtigen, wenn die Einhaltung der erklärten Verpflichtung nicht mehr gewährleistet werden kann, insbesondere, wenn für ihn eine Notwendigkeit oder Verpflichtung entsteht oder er eine solche hätte erkennen können, die ihn an der Einhaltung dieser Verpflichtung hindern könnte.
7. Der Hersteller verpflichtet sich, auf Anfrage konkrete Angaben über die Produktentwicklung der sicherheitsrelevanten Systemanteile seiner Produkte zu machen.
8. Der Hersteller verpflichtet sich, für die Entwicklung und Herstellung der sicherheitskritischen Systemanteile nur besonders vertrauenswürdige Mitarbeiter einzusetzen.
9. Der Hersteller verpflichtet sich, auf Anfrage und gegen entsprechende Vertraulichkeitszusage sämtliche Produktunterlagen zu einem Produkt inkl. Source Code, Hardware Konstruktionsunterlagen, Prüfwerkzeuge, Debug-Versionen etc. im vollen Umfang zur Verfügung zu stellen, um erforderliche Sicherheitsanalysen zu ermöglichen.
10. Der Hersteller erklärt sich bereit, Sicherheitsüberprüfungen und Penetrationsanalysen im erforderlichen Umfang an seinem Produkt zuzustimmen und in angemessener Weise zu unterstützen.
11. Der Hersteller versichert, dass das Produkt, für dass die Erklärung abgegeben wird, keine vorsätzlich implementierten Schwachstellen besitzt und dass diese zu keinem späteren Zeitpunkt eingebaut werden sowie dass alle bekannten unbeabsichtigten Schwachstellen behoben worden sind oder in Zukunft kurzfristig beseitigt werden, sowie dass das Produkt frei von von Dritten eingebrachten Funktionsmerkmalen ist.
12. Der Hersteller verpflichtet sich, dass er ihm bekannte bzw. bekannt gewordene Schwachstellen oder Manipulationen unverzüglich dem Bedarfsträger meldet, sodass

frühzeitig Maßnahmen zur Eingrenzung und Beseitigung möglicher Folgewirkungen von Qualitätsmängeln ergriffen werden können. Auf Anfrage teilt der Hersteller alle ihm bekannten Anwender seines Produkts bei den Stellen des Bundes mit. Gelangt der Hersteller an Informationen, die die Sicherheit und Funktion seiner Produkte schwächen oder die einen bestimmungsgemäßen Betrieb negativ beeinflussen können, so wird dies dem Bedarfsträger unverzüglich mitgeteilt. Weiterhin verpflichtet sich der Hersteller zur unmittelbaren Bereitstellung von Lösungsvorschlägen.

13. Der Hersteller stimmt Überprüfungen vor Ort zu den in der Erklärung angegebenen Tatsachen zu.