Allgemeines

2

2.1 Allgemeine Herausforderungen in Bezug auf die IT-Sicherheit

Das Thema IT-Sicherheit ist in der Mitte der Gesellschaft angekommen. Kaum eine Woche vergeht, in der die Medien nicht über einen spektakulären Cyberangriff oder andere Attacken auf die IT berichten und über die Notwendigkeit betrieblicher und individueller Abwehrmaßnahmen zum Schutz der privaten und öffentlichen Infrastruktur informieren. Dies erfolgt vor dem realen Hintergrund, dass die tiefe strukturelle Abhängigkeit der Gesellschaft von IT und vom Internet eine sensible Angriffsfläche für kriminelle Aktivitäten bildet. Im Zuge der flächendeckenden digitalen Vernetzung sind von Cyberattacken in wachsendem Ausmaß neben den kritischen Infrastrukturen und öffentlichen Einrichtungen vor allem konventionelle Infrastrukturen in Unternehmen und privaten Haushalten betroffen, deren Ausfall eine immense Einschränkung des öffentlichen und privaten Lebens und einen erheblichen finanziellen Schaden und/oder Vertrauensverlust für die Unternehmen und Privatpersonen darstellen kann. Erfolgte Schadensfälle und Reparaturmaßnahmen sind oft mit hohen Aufwänden verbunden, die in Form direkter und indirekter Kosten für Unternehmen, öffentliche Organisationen und Privatpersonen anfallen, wenngleich diese oft schwer zu quantifizieren sind. Entsprechend ist in vernetzten Gesellschaften ein deutlich größeres und differenziertes Augenmerk auf Maßnahmen zu legen, die Cyberbedrohungen präventiv abwehren. Dies beginnt insbesondere bei der Beschaffung von Hard- und Software.

Daher sind bei der Beschaffung von Hard- und Software die Vertrauenswürdigkeit des Herstellers und die IT-Sicherheit des Produkts von sehr großer Bedeutung. Einerseits sollen Hersteller bzw. Anbieter (Händler, Lieferanten)

E. Piller, *Beschaffung unter Berücksichtigung der IT-Sicherheit,*
essentials, DOI 10.1007/978-3-658-18599-2_2

ihren Kunden garantieren können, dass die angebotene Hardware und/oder Software ordnungsgemäß funktioniert, die relevanten und wichtigen IT-Sicherheitsanforderungen erfüllt und keine bewussten Fehler oder Schwachstellen besitzt. Andererseits müssen verantwortungsvolle Kunden versuchen, im Rahmen einer „IT-sicheren Beschaffung“ darauf zu achten, dass die erworbenen Produkte IT-sicher und vertrauenswürdig sind und nur die gewünschten Funktionalitäten enthalten. Nur dann kann man diese Produkte ohne Vorbehalt einsetzen, vor allem für sicherheitskritische Aufgaben, und eventuell vorhandene rechtliche, Compliance oder sonstige Vorgaben erfüllen.

IT-Sicherheit wird zunehmend ein wichtiges Thema in der Politik, vor allem durch die Zunahme der gezielten Angriffe (Spionage, Sabotage) auf staatliche Einrichtungen und kritische Infrastrukturen, die vermehrt von Staaten selbst mit hohen Budgets durchgeführt werden (siehe Abschn. 4.5). Die heute vorhandene strenge und zum Teil überbordende Gesetzgebung in der „Analogwelt“, wie im Gesundheitswesen, Industrieumfeld, Autoverkehr, beim Brandschutz etc. ist in der „Digitalwelt“ noch überhaupt nicht angekommen. Aber ohne Gesetze und Vorschriften wird von den Herstellern und Anwendern kein adäquates IT-Sicherheitsniveau garantiert werden können, was nicht bedeutet, dass man dazu die Vielzahl der „Analogwelt“ benötigt. Und ohne ausreichende IT Sicherheit kann keine nachhaltige Digitalisierung gelingen. Nicht einmal die einfachsten Schutzmaßnahmen wie Virenscanner, Firewalls etc. und IT-Sicherheitsanforderungen wie sichere Passwörter, Zugriffskontrolle, Vertraulichkeit etc. sind heute, von einzelnen Ausnahmen abgesehen, direkt vorgeschrieben. Das deutsche Manifest zur IT-Sicherheit [72] mit sechs wichtigen Thesen stellt fest, dass IT-Security-by-Design und Privacy-by-Design unabdingbar sind. Das Manifest ruft auf, dass die Gesellschaft intolerant gegenüber unsicheren IT-Lösungen sein muss und dass wir vom angebotsgetriebenen zum anforderungsgetriebenen IT-Sicherheitsmarkt kommen müssen. Dazu sollen die Anwender gemeinsam ihre Beschaffungsmacht fair nutzen, d. h. über die Beschaffung die IT-Sicherheit deutlich verbessern. Das Manifest erteilt auch einer staatlich motivierten Schwächung von Kryptografie und den Wünschen nach Hintertüren eine Absage und fordert, dass die EU kurz- bis mittelfristige Maßnahmen ergreifen muss, um die Souveränität im Bereich IT-Sicherheit aufzubauen und zu sichern.

Es stellt sich die Frage, ob die IT-sichere Beschaffung auch zur Durchsetzung politischer Ziele dienen soll, wie z. B. im Bereich Umwelt. In Deutschland sieht der § 97 IV GWB vor, dass Beschaffer für die Auftragsausführung zusätzliche Anforderungen an Auftragnehmer stellen können, die insbesondere soziale, umweltbezogene oder innovative Aspekte betreffen. Dabei fehlt noch der sehr wichtige IT-Sicherheitsaspekt, sofern man ihn nicht bereits unter innovative

Aspekte führt. Aus den Formulierungen der umweltbezogenen Aspekte kann man eine Erweiterung auf IT-Sicherheitsaspekte ableiten. Z. B. werden unter dem Begriff „Green-IT“ alle Maßnahmen verstanden, die dazu führen, ein IKT-Produkt über seinen gesamten Lebenszyklus hinweg so ressourcenschonend und umweltfreundlich wie möglich zu gestalten und zu nutzen. Daher soll der Begriff „Secure IT“ ein wichtiger Begriff jedes Beschaffungsvorganges werden und Gütezeichen wie z. B. IT Security Made in Germany, Made in Austria, Made in Switzerland an Bedeutung gewinnen, wie sie heute schon in der Lebensmittelindustrie üblich sind. In diese Richtung geht auch eine Forderung des SPD-nahen Vereins D64 nach einem europäischen Gütesiegel für abhörfreie Technik und einem Einfuhrverbot von Hardware aus den USA und anderen Ländern, die nicht europäische IT-Sicherheitsstandards erfüllt – dazu müssen aber vorher diese IT-Sicherheitsstandards gesetzlich vorgeschrieben werden. Mit dieser Forderung bzw. einem Gütesiegel können Produkte aus dem eigenen Land oder aus Mitteleuropa deutlich aufgewertet werden. Dies ist gerade in der IT-Sicherheit möglich, wo Vertrauen eine große Rolle spielt und dieses Vertrauen derzeit zum Teil gestört ist, weil einzelne Staaten und Hersteller nachweislich IT-Sicherheitsschwachstellen in Produkte einbauen oder einbauen lassen.

Es ist wohl nicht übertrieben zu behaupten, dass alle Nutzer von IKT zu einem gewissen Grad von ihren Anbietern bzw. Herstellern abhängen. Die meisten IKT-Produkte spielen eine kritische Rolle in den Geschäfts- und Verwaltungsprozessen ihrer Nutzer. Es besteht daher ein großer Bedarf für Beschaffer IT-Sicherheitsrisiken sorgfältig zu managen und die richtigen IT-Sicherheitsmaßnahmen festzulegen, um eine gleichbleibende Widerstandsfähigkeit in ihrer eigenen Infrastruktur bzw. bei Produktionsunternehmen bei ihren produzierten Produkten sicherzustellen. Dies bedeutet, dass alle Beteiligten in einem Beschaffungsprozess zusammenarbeiten sollen, und dazu gehören neben den Beschaffern auch IT-Sicherheitsexperten, zumindest IT-Experten. Da dies nicht immer möglich ist bzw. diese Experten nicht zu Verfügung stehen, kann eine professionelle Beschaffungsplattform wichtige Dienste leisten.

Die Lieferketten von Hard- und Software werden immer globaler und komplexer und bringen große Herausforderungen und Abhängigkeiten für Hersteller, Anbieter und Endkunden mit sich. Mehrere Komponenten, die in verschiedenen Ländern entworfen, entwickelt und hergestellt werden, werden kombiniert, um daraus eine einzige Hardware oder Software zu produzieren, die später von einem Beschaffer über einen einzigen Anbieter erworben werden. Jeder Akteur der globalen Produktlieferkette hat die Verantwortung, die erforderliche IT-Sicherheit und die Widerstandsfähigkeit des Produkts vor Angriffen von außen zu gewährleisten. Durch die Komplexität des Produkts und der Lieferkette ist eine effektive

Gewährleistung und Überprüfung einer definierten IT-Sicherheit in vielen Fällen aber gar nicht möglich. Dadurch entsteht das Risiko, dass Beschaffer oftmals das IT-Sicherheitsniveau und die IT-Sicherheitsschwachstellen der Produkte nicht kennen und keine oder nur eine beschränkte Rückverfolgbarkeit und Kontrolle über die eigenen Produkte haben. Sie kaufen möglicherweise Produkte mit integrierter Sabotage- oder Spionage-Funktion, bewussten Schwachstellen, nicht ausreichendem Zugriffs- und Datenschutz, mangelhafter Protokollierung etc.

Hersteller, die Hard- und Software nach international üblichen IT-Sicherheitsanforderungen und Standards entwickeln und ein hohes IT-Sicherheitsniveau garantieren, können dies oftmals als Alleinstellungsmerkmal gegenüber Kunden anführen und daraus einen Wettbewerbsvorteil generieren. Doch viele IT-Sicherheitsmaßnahmen sind aus wirtschaftlicher bzw. unternehmerischer Perspektive ein Kostenfaktor. Dies führt oftmals dazu, IT-Sicherheitsmaßnahmen nur minimalistisch einzuführen bzw. in Extremfällen ganz darauf zu verzichten. Das kann natürlich bei Anbietern für die Gesellschaft kritischer Leistungen so nicht akzeptiert werden und es muss darauf gedrängt werden, dass IT-Sicherheit bedacht wird und in ausreichende IT-Sicherheit investiert wird. Dies zeigt sich gerade in der Diskussion, ob erforderliche IT-Sicherheitsmaßnahmen gesetzlich bzw. regulatorisch eingefordert werden können (siehe oben) oder ob diese nur auf Basis einer freiwilligen Selbstverpflichtung, z. B. in Form sogenannter „Managed Security Services“, erbracht werden sollen [66].

In Summe bleibt festzuhalten, dass heute die Beschaffung von Hard- und Software mit folgenden Herausforderungen in Bezug auf die IT-Sicherheit konfrontiert ist:

- Steigende technische Komplexität der zu sichernden Infrastruktur, Software und Hardware (mit integrierter Software).
- Sinkende Möglichkeiten der lückenlosen Überprüfbarkeit der IT-Sicherheit bestehender Infrastrukturen und den darauf basierenden Komponenten.
- Widersprüchliche wirtschaftliche Logiken und Funktionsprinzipien zwischen Anbietern und Beschaffern.
- Bewusste Integration von IT-Sicherheitsschwachstellen von Herstellern während des Produktdesigns bzw. der Produktentwicklung, die zum Teil von Staaten gefördert bzw. gefordert wird.
- Zum Teil fehlendes Know-how sowie methodische Frameworks zur Lösung der oben beschriebenen Herausforderungen.

2.2 IT-sicherheitsspezifische Herausforderungen bei der Beschaffung

Ein Bericht der ENISA (European Union Agency for Network and Information Security) [60] identifiziert sechs IT-sicherheitsspezifische Herausforderungen bei der Beschaffung von Hard- und Software. Dazu gehören:

Fehlende Angemessenheit und Wirksamkeit der IT-Sicherheitsziele und Kontrollen aufseiten des Anbieters bzw. Herstellers

- Die IT-Sicherheitsziele der Anbieter bzw. Hersteller sind nicht mit den IT-Sicherheitsanforderungen der Beschaffer in Einklang zu bringen, um bekannte IT-Sicherheitsrisiken zu verhindern und das gewünschte IT-Sicherheitsniveau der Kunden (Beschaffer) zu erreichen.
- Anbieter wollen Beschaffern oftmals keine Zusicherung gewähren, dass relevante Kontrollen vorhanden sind und ordnungsgemäß funktionieren, um die von Beschaffern festgelegten IT-Sicherheitsmindestanforderungen zu erfüllen.

Management potenzieller Anfälligkeiten durch (unbekannte) Schwachstellen

- Fehlen aktueller und zeitkritischer Information zu Schwachstellen, die sich auf das Produkt, die Dienstleistung bzw. auf Prozesse auswirken, insbesondere, dass Anbieter so schnell wie möglich informieren, wenn ein anderer Anbieter oder Kunde Probleme mit denselben Produkten hat.
- Haftung seitens des Anbieters oder seiner Lieferanten (Zulieferer), insbesondere des Herstellers, für IT-Sicherheitsschwachstellen sowie für geringe Qualität, fehlende Kontrollen oder fehlerhafte Software.

Die Nichteinhaltung der im Vertrag auf der Seite des Anbieters festgelegten IT-Sicherheitsanforderungen

- Dem Beschaffer ist es nicht immer möglich die Einhaltung der vereinbarten Vertragsbedingungen zu kontrollieren.

Angemessene Unterstützung durch den Anbieter im Falle einer Panne

- Potenzieller Mangel an Unterstützung von Anbietern bei Zwischenfällen.
- Angemessene Reaktionszeiten und Bereitstellung qualifizierter Fachleute zur Beseitigung von Zwischenfällen seitens des Anbieters.

Schwache Verhandlungsstärke des Beschaffers zur Erzwingung bestimmter IT-Sicherheitsanforderungen

- Inhärenter Mangel an Verhandlungsmacht seitens der Beschaffer, da die Alternativen auf dem Markt oftmals begrenzt sind.
- Problem der Erhöhung der Kosten seitens der Anbieter bzw. Verzögerungen im Time-to-Market, wenn zusätzliche IT-Sicherheitsmaßnahmen seitens des Beschaffers gefordert werden.

Fehlende Rahmenbedingungen oder Richtlinien, um Anbieter durch einen Beschaffungsprozess zu führen

- Trotz existierender Standards fehlen ein integrierter und einheitlicher Ansatz und korrespondierende Richtlinien, die insbesondere Beschaffer bei der gezielten Behandlung von IT-Sicherheitsrisiken im Beschaffungsprozess unterstützen.

http://www.springer.com/978-3-658-18598-5

Beschaffung unter Berücksichtigung der IT-Sicherheit
Wichtigkeit, Herausforderungen und Maßnahmen
Piller, E.
2017, XIII, 58 S. 4 Abb., Softcover
ISBN: 978-3-658-18598-5