View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

Zertifizierter Datenschutz in Europa möglich

Ergebnisse aus dem Projekt EuroPriSe

von Jaro Sterbik-Lamina und Walter Peissl, ITA Wien

Zur Verhinderung von Kriminalität und zur Abwehr von Terrorgefahr wird von Politikern immer häufiger eine erweiterte Überwachung gefordert, die auch in die Privatsphäre unbeteiligter Personen eingreifen kann. Sicherheit und Datenschutz müssen einander aber nicht ausschließen – der Einsatz cleverer Technik kann beides verbinden. Dieses Jahr ist unter der Leitung des Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein das Projekt „European Privacy Seal" (EuroPriSe)[1] zu Ende gegangen, das im Rahmen des „eTEN-Programms" von der Europäischen Kommission im Projektzeitraum 2007 bis 2009 gefördert wurde. Im Zuge der Arbeit an dem Projekt sind viele interessante Fragen aufgetaucht und beantwortet worden: „Wie erfolgreich war die Datenschutzrichtlinie aus dem Jahr 1995 in der Harmonisierung des Datenschutzniveaus innerhalb der Europäischen Union?" „Ab wann ist Datenschutz wirtschaftlich interessant?" Oder „lässt sich mit der Einhaltung von Grundrechten Geld verdienen"?

1 Vorbild Schleswig-Holstein

Ausgangspunkt für das Projekt EuroPriSe im Rahmen des eTEN-Programms[2] (EC 2009) der Europäischen Union war ein bereits etabliertes Datenschutzgütesiegel in Schleswig-Holstein, das vom dortigen Unabhängigen Landeszentrum für Datenschutz seit Jahren vergeben wird. Aufgrund der föderalen Datenschutzgesetzgebung (in Deutschland) konnte es aber nur wenig über die Grenzen des Bundeslandes hinaus wirksam werden. Zugleich muss man festhalten, dass seit Bestehen des Schleswig-Holstein'schen Gütesiegels zahlreiche Zertifikate ausgestellt werden konnten, dass sich auch große, internationale Unternehmen (wie beispielsweise Microsoft) darum bemüht haben, und dass es im nördlichsten Bundesland Deutschlands sogar insofern einen gesetzlichen Niederschlag fand, als öffentliche Stellen bei der Evaluierung von Produkten im Rahmen des Beschaffungswesens jene mit dem Gütesiegel zu bevorzugen haben. Dadurch bestehen natürlich für Unternehmen zusätzliche Anreize, ihre Investitionen in den Datenschutz in ihren Produkten sichtbar zu machen.

2 Ziele des europäischen Projekts

Das Projekt EuroPriSe hatte mehrere Aufgaben zu erfüllen. Einerseits sollte geklärt werden, ob es eine gemeinsame europäische Basis geben kann, auf der ein Zertifizierungsschema zum Datenschutz in Produkten und IT-Services fußen kann, und wie diese auszusehen hätte. Damit einhergehend mussten Prozesse für eine europäische Akkreditierung von ExpertInnen und unabhängigen Zertifizierungsstellen erarbeitet werden, die einen durchgängig hohen Standard („Seal of Excellence") in den Zertifizierungen gewährleisten. Andererseits musste unter den wichtigsten AkteureInnen am Markt geklärt werden, ob überhaupt ein Bedarf für diese Dienstleistung besteht – sowohl auf Seite der ProduzentInnen als auch der KonsumentInnen, und ob es MarktteilnehmerInnen gibt, die bereit wären, diese Dienstleistung anzubieten.

Um die erstgenannte Aufgabe zu erfüllen, wurden Kriterien erstellt und im Laufe des Projekts mehrmals überarbeitet, die die Grundlage für eine Evaluierung eines Produkts oder einer Dienstleistung in diesem Rahmen abstecken (Bock et al. 2009). Ausgangspunkt dazu war die Datenschutzrichtlinie der Europäischen Union[3], die den gemeinsamen datenschutzrechtlichen Rahmen für alle Mitgliedsstaaten bildet, und auf die die aktuellen Datenschutzgesetze aller EU-Staaten Bezug nehmen. Ergänzend dazu wurden die Urteile des Europäischen Gerichtshofes zu Datenschutzfragen sowie die Stellungnahmen der „Article 29 Working Party" ausgewertet, die das offizielle Gremium für Interpretationen der Richtlinie darstellt und sich aus VertreterInnen aller Datenschutzbehörden der einzelnen Mitgliedsstaaten zusammensetzt. Darüber hinaus wurden andere, sektorale europäische Bestimmungen, wie die Telekomrichtlinie[4], berücksichtigt. Auf unterschiedliche Implementierungen der Datenschutzrichtlinie in den einzelnen Nationalstaaten wird im Kriterienkatalog eingegangen,

im Wesentlichen bleibt es aber den ExpertInnen im jeweiligen Land überlassen, das zu beurteilen.

Auf der Grundlage der genannten Quellen ergibt sich auch die Definition dessen, was durch das Europäische Datenschutzgütesiegel zertifiziert wird: „The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States." (Bock 2009, S. 5)

3 Projektablauf

Das Projekt EuroPriSe wurde in mehreren, teilweise parallel laufenden Arbeitsschritten durchgeführt. Zu Beginn der Markterhebung stand ein Fragebogen, der sowohl an Hersteller (also KundInnen aus Sicht des Zertifizierungsprozesses) als auch potenzielle EvaluatorInnen (Expert Innen auf den Gebieten Recht und / oder Informationstechnik) versandt wurde. Zeitgleich wurde ein Zertifizierungsschema ausgearbeitet. Um für die Pilotphase ExpertInnen zu akkreditieren, wurden insgesamt zwei Workshops abgehalten, die beide bis an die Kapazitätsgrenzen gebucht wurden und damit alle Erwartungen betreffend das Interesse am Markt übertrafen.

Die Pilotphase, in der Produkte und Dienstleistungen zertifiziert werden konnten, wurde in zwei Calls ausgeschrieben. Alle verfügbaren Plätze waren innerhalb kurzer Zeit vergeben. Sowohl ExpertInnen als auch Pilot-KundInnen wurden nicht nur in Ländern, in denen Projektpartner tätig waren, sondern auch in einigen anderen Staaten Europas gefunden.

Auch wenn das Interesse an der Teilnahme an Pilotzertifizierungen überaus groß war, mussten einige wenige Firmen ihr anfängliches Interesse jedoch zurückziehen. Die Gründe dafür waren ganz unterschiedlich: Einmal wechselte das Management während der Vorgespräche, sodass dann andere Punkte firmenintern vorgereiht wurden. Ein anderes Mal gab es unterschiedliche Auffassungen über die Notwendigkeit einer Zertifizierung zwischen Betrieb, Marketing und Management. Und natürlich waren vor allem für kleine Unternehmen die Kosten der Evaluierung ein wichtiges Argument. Auch wenn sich die Zertifizierung im Laufe der Zeit rentieren würde, können die auflaufenden Kosten einen Liquiditätsengpass hervorrufen und deshalb limitierend wirken.

Generell war festzustellen, dass Firmen, die schon in anderen Bereichen auditiert oder zertifiziert wurden, dem Projekt aufgeschlossener gegenüberstanden, und dass ein höherer organisatorischer Reifegrad des Unternehmens sich sehr positiv auf die zu erwartenden (internen) Kosten auswirkt, weil dadurch bestimmte Vorgaben (getrennte Verantwortungsbereiche, Prozessdokumentationen, Kontrollmechanismen und dergleichen mehr) bereits umgesetzt sind. Das wiederum hatte zu einer höheren Bereitschaft geführt, im Rahmen des Projekts eine Zertifizierung zu versuchen.

4 Auf dem Weg zum Gütesiegel

Das Schema, nach dem eine Zertifizierung abläuft, sieht vier Schritte bis zur Verleihung des Gütesiegels vor:

1. Das Unternehmen, das ein Produkt oder eine Dienstleistung zertifiziert haben möchte, entscheidet sich für zwei ExpertInnen aus einer Liste akkreditierter EuroPriSe-EvaluatorInnen, die auf der Projekt-Webseite eingesehen werden kann. Es muss mindestens ein / eine Rechtsexperte / -expertin und ein / eine technische(r) Experte / Expertin gewählt werden. Gemeinsam wird der Rahmen für die Evaluierung („Target of Evaluation", ToE) festgelegt und bei der Zertifizierungsstelle eingereicht.
2. Nach der Einigung auf ein ToE beginnen die ExpertInnen an Hand der EuroPriSe-Kriterien die Datenverarbeitung im Zuge der zu überprüfenden Dienstleistung oder des Produkts zu untersuchen. Dabei soll festgestellt werden, ob alle Vorgaben der europäischen Datenschutzbestimmungen eingehalten und ob die Daten entsprechend eines strikten Informationssicherheitsmanagements verarbeitet werden.
3. Die ExpertInnen geben ihren Bericht an den Hersteller, der nun darüber entscheiden kann, ob er ihn bei der Zertifizierungsstelle einreicht. Im Falle einer Einreichung überprüfen MitarbeiterInnen der Zertifizierungsstelle den Bericht auf Vollständigkeit, Methodik und Plausibilität. Bei Unklarheiten

oder Mängeln in der Ausführung des Berichts müssen die ExpertInnen entsprechend nachbessern, bis sich ein Gesamtbild ergibt, nach dem die Zertifizierungsstelle entscheiden kann, ob eine Vergabe des Gütesiegels gerechtfertigt ist oder nicht.

4. Im Falle einer positiven Beurteilung wird das Gütesiegel mit einer Gültigkeit von zwei Jahren an den Antragsteller verliehen. Danach erlischt es, oder der Hersteller unterzieht das Produkt einer Rezertifizierung. Ein öffentlich einsehbarer Kurzbericht über das Produkt und das Prüfergebnis wird auf der EuroPriSe-Webseite veröffentlicht.[5]

5 Ziele des Gütesiegels

Mit dem Zertifizierungsprozess wurden mehrere Ziele verfolgt. Zum einen wurde ein Konstrukt in einen bis dahin nahezu unerschlossenen und unstrukturierten Markt gesetzt, an dem sich andere Initiativen in Zukunft ausrichten können und messen lassen müssen, und das somit zur Markterschließung beigetragen hat – was ja auch eines der Ziele des eTEN-Programms war. Zum anderen wurde der Brückenschlag von den in vielen Bereichen üblichen Zertifizierungen (beispielsweise ISO 9000 / Qualität, ISO 27000/ Informationssicherheit, ISO 15408 / Common Criteria u. v. m.) zum Bereich Datenschutz geschafft. Damit ist es Unternehmen möglich, ihre Investitionen in Datenschutz und Datensicherheit auch für den Endverbraucher sichtbar zu machen. Es ist auch ein weiterer Schritt, um Datenschutz von einem rechtlich notwendigen Kostenfaktor zu etwas zu machen, das man sich als Hersteller auch aus wirtschaftlichen Überlegungen genauer ansehen sollte. Wenn es ausschließlich um Zahlen gehen soll, kann man den sogenannten „Return on Security Investment" (ROSI) berechnen und so auch quantitativ nachweisen, dass Datenschutz auch ökonomisch Sinn macht. Das Ergebnis wird in jedem Unternehmen anders ausfallen.

Wichtig scheint das „Sichtbar-Machen" des Datenschutzinvestments, das noch andere Entwicklungen unterstützen soll: Einerseits soll das Bewusstsein für Datenschutz und Privatsphäre bei den VerbraucherInnen steigen. Andererseits soll diesen bei der Kaufentscheidung geholfen werden, da es nicht allen KonsumentInnen zumutbar oder möglich ist, selbst genau festzustellen, wie bei einem beliebigen IT-Produkt oder -Service mit ihren Daten verfahren wird.

Dieses Projekt hat gezeigt, dass Selbstregulierungsbestrebungen des Marktes auch unter Einbeziehung öffentlicher Partner und Non-Profit-Organisationen erfolgreich umgesetzt werden können. Inhaltlich ist dieser Prozess vor allem deshalb interessant, weil er zeigt, dass aus dem Markt heraus eine Initiative zum Schutz der Daten der Konsumenten in ein erfolgreiches Projekt münden konnte. Nicht zuletzt auch deswegen, weil man in der Wirtschaft immer öfter erkennt, dass Datenschutz Vertrauen schafft und obendrein hilft, Schäden vom Unternehmen fernzuhalten, sich also abseits aller gesellschaftspolitischen Überlegungen rein finanziell auszahlt.

Hier lässt sich auch erkennen, dass Datenschutz und Wirtschaftlichkeit keine Gegensätze sind. Weder müssen Maßnahmen zur Förderung des Datenschutzes immer kostspielig sein, noch ist es so, dass sie einen reinen Kostenfaktor darstellen, und nicht zum finanziellen Ergebnis eines Unternehmens positiv beitragen könnten.

6 Ergebnis

Die grundsätzliche Frage bei der im Rahmen des Projekts durchgeführten Markterhebung, nämlich ob es einen Markt in Europa für eine derartige Zertifizierung gibt, lässt sich aus heutiger Sicht mit einem klaren „Ja" beantworten. Das Interesse an dem Projekt war von allen Seiten deutlich größer als erwartet und ein Business Plan des ULD Schleswig-Holstein legt nahe, dass es möglich sein wird, dieses Zertifizierungsschema über die nächsten Jahre kommerziell anzubieten.

Um die eingangs gestellten Fragen aus den im Projekt gewonnenen Erfahrungen zu beantworten: Ja, die Harmonisierung des Datenschutzes ist grundsätzlich gelungen, sodass man von einem europäischen Datenschutzniveau sprechen kann. Allerdings ist die Ausformung in den einzelnen Nationalstaaten so unterschiedlich, dass es bei einer Zertifizierung wie dieser notwendig scheint, nach der allgemeinen Prüfung genau das Recht des jeweiligen Mitgliedslandes anzusehen, um eine vollständige Konformität mit lokalen Vorschriften zu gewährleisten. Abgesehen davon werden sowohl auf EU-Ebene, als auch in den einzelnen Ländern gerade viele

Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre der BürgerInnen überarbeitet. Wenn diese Welle der Erneuerung abgeschlossen ist, wird man sehen müssen, ob die gesetzlichen Vorgaben nach wie vor dieses relativ einheitliche Bild zeigen.

Darüber hinaus ist zu bemerken, dass, aufgrund der in manchen Bereichen sehr allgemeinen Formulierungen, die Richtlinie alleine nicht ausreichend wäre, um ein „europäisches Datenschutzniveau" zu definieren. Sehr viel Interpretationsarbeit wird hier von der „Article 29 Working Party" geleistet. Daher ist es notwendig, deren Erkenntnisse, sowie die des Europäischen Gerichtshofes, mit einzubeziehen.

Die Frage, ob Datenschutz über das gesetzlich vorgeschriebene Maß hinaus, wirtschaftlich interessant ist, muss jedes Unternehmen für sich beantworten. Es gibt verschiedene Modelle, die den ROSI berechnen. Teil all dieser Berechnungen ist aber immer die Abschätzung der jeweiligen Folgekosten, falls es zu einem Schadensfall kommt, der durch eine bessere Informationssicherheitspolitik hätte verhindert werden können. Dazu zählen dann auch schwer quantifizierbare Größen wie der Imageschaden, den ein Unternehmen durch einen derartigen Vorfall davontragen kann. Natürlich müssen auch strategische Überlegungen zum Marketing mit einfließen. Wenn die Gruppe der potenziellen KundInnen auf diese Problematik bezogen sehr gut informiert ist oder die Marktbegleiter im jeweiligen Segment alle eine Zertifizierung ihres Produkts anstreben, kann es unumgänglich werden, den Weg über eine Zertifizierung zu gehen.

Lässt sich mit der Einhaltung von Grundrechten Geld verdienen? Auch das lässt sich mit einem „Ja" beantworten. Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein hat bereits mit der lokalen Version des Gütesiegels gezeigt, dass das im kleinen Rahmen funktioniert – sowohl für Hersteller, als auch ExpertInnen und Zertifizierungsstellen. Die Erfahrungen des Konsortiums aus dem EuroPriSe-Projekt legen nahe, dass das auch auf europäischer Ebene möglich sein wird.

Anmerkungen

1) https://www.european-privacy-seal.eu/
2) „Das eTEN-Programm der Europäischen Gemeinschaft fördert die Bereitstellung innovativer, transeuropäischer elektronischer Dienste, die im gesellschaftlichen und wirtschaftlichen Interesse liegen." (EC 2009) Innerhalb dieses Rahmens wurden Projekte zu verschiedenen Themen bezuschusst, unter anderen zum Thema „Vertrauen und Sicherheit", worunter auch das EuroPriSe-Projekt gefallen ist. Im Rahmen des Programms konnten sowohl Markteinführungen als auch Marktvalidierungen durchgeführt werden.
3) Richtlinie 95 / 46 / EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
4) Richtlinie 2002 / 58 / EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.
5) Im Falle einer negativen Beurteilung eines eingereichten Berichts wird nur der Antragsteller über das Ergebnis informiert.

Literatur

Bock, K., 2009: European privacy Seal – Final report. Im Auftrag von European Commission – eTEN, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD Kiel); https://www.european-privacy-seal.eu/results/deliverables/Final%20Report (download 17.9.09)

Bock, K.; Meissner, S.; Storf, K., 2009, Description of EuroPriSe Criteria and Procedures (updated Version 1.1). Im Auftrag von European Commission – eTEN, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD Kiel); https://www.european-privacy-seal.eu/results/deliverables/procedures (download 17.9.09)

EC – European Commission, 2009: eTEN Brochure (German). http://ec.europa.eu/information_society/activities/eten/library/about/brochure/index_de.htm (download 17.9.09)

Kontakt

Jaro Sterbik-Lamina, MSc
E-Mail: jsterbik@oeaw.ac.at

Dr. Walter Peissl
E-Mail: wpeissl@oeaw.ac.at

Institut für Technikfolgen-Abschätzung
Österreichische Akademie der Wissenschaften
Strohgasse 45/5, A-1030 Wien
Internet: http://www.oeaw.ac.at/ita

« »