ISSN: 1977-9119

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

EDSB Newsletter

N 41 | April 2014

IN DIESER AUSGABE

SCHLAGLICHTER

1 Gleiche Regeln für alle: Die EU-Datenschutzreform kann die Wirtschaft fördern und Bürger schützen

1 Durchsetzung des europäischen Datenschutzrechts ist unerlässlich, um das Vertrauen zwischen der EU und den Vereinigten Staaten wiederherzustellen

2 EDSB: Aktive Aufsicht hält die EU-Einrichtungen beim Datenschutz auf dem richtigen Weg

AUFSICHT

2 Menschlicher Fehler führt zu Sicherheitsverletzungen

2 Das neue Statut der EU-Beamten und die Weiterverarbeitung von Personalbeurteilungen

2 ARACHNE: Kein Spinnennetz für den Datenschutz

3 Videoüberwachung: Der EDSB begrüßt Verbesserungen bei Einrichtungen der EU

BERATUNG

3 Fortschritte beim Datenschutzreformpaket

3 Zahlungen im Binnenmarkt

4 Unterbindung des illegalen Handels mit Schusswaffen muss Datenschutzziele berücksichtigen

4 Datenabgleich zur Bekämpfung von grenzüberschreitendem Sozialversicherungsbetrug benötigt Datenschutzgarantien

4 Schutz personenbezogener Daten in der Nahrungsmittelkette

IT POLICY

5 Internettechniker diskutieren über besseren Schutz der Privatsphäre und mehr Sicherheit

5 Wird mobile Sicherheit zur entscheidenden Herausforderung für die Privatsphäre?

VERANSTALTUNGEN

6 Eröffnung des EDSB-Labors im Frühjahr

VORTRÄGE UND VERÖFFENTLICHUNGEN

BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

SCHLAGLICHTER

Gleiche Regeln für alle: Die EU-Datenschutzreform kann die Wirtschaft fördern und Bürger schützen

Die Reform der EU-Datenschutzregeln wird die sich erholende, aber immer noch fragile europäischen Wirtschaft fördern, erklärte der Europäische Datenschutzbeauftragte (EDSB) nach der Vorstellung seines Jahresberichts für das Jahr 2013 im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments. Die überarbeiteten Regeln sollen für Klarheit und Kohärenz in ganz Europa sorgen: Die gleichen Regeln werden für alle Unternehmen, die in der EU Geschäfte tätigen, gelten, unabhängig davon, wo sie ihren Sitz haben, und die Bürger werden mehr Vertrauen dazu haben können, wie ihre Daten genutzt werden.

Das Europäische Parlament hat mit überwältigender Mehrheit für das Reformpaket gestimmt; dieses Paket besteht aus einem einheitlichen Satz von Regeln, deren Befolgung sowohl für Online- und traditionelle Unternehmen einfacher - und wirtschaftlicher - sein wird. Es ist nun Sache des Rates, das gesamte Paket zu unterstützen, damit die Bürger das Recht haben, zu kontrollieren, wie ihre personenbezogenen Daten genutzt werden, und Regressansprüche, wenn sie unfair behandelt oder diskriminiert werden.

Peter Hustinx, EDSB

Jahresbericht 2013 des EDSB

Pressemitteilung des EDSB

Durchsetzung des europäischen Datenschutzrechts ist unerlässlich, um das Vertrauen zwischen der EU und den Vereinigten Staaten wiederherzustellen

Die strikte Durchsetzung des bestehenden europäischen Datenschutzrechts ist ein unerlässliches Element, um das Vertrauen zwischen der EU und den USA wiederherzustellen, erklärte der Europäische Datenschutzbeauftragte (EDSB) nach der Veröffentlichung seiner Stellungnahme am 20. Februar 2014.

Die Rechte der EU-Bürger auf den Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten sind im EU-Recht verankert. Die massenhafte Überwachung von EU-Bürgern durch US- und andere Geheimdienste ignoriert diese Rechte. Zusätzlich zur Unterstützung eines allgemeinen Datenschutzgesetzes in den USA muss Europa auf der strikten Durchsetzung von EU-Recht bestehen, internationale Datenschutzstandards voranbringen und die Reform der EU-Datenschutzverordnung zügig abschließen. Es sind gemeinsame Anstrengungen erforderlich, um das Vertrauen wiederherzustellen.

Peter Hustinx, EDSB

Stellungnahme des EDSB

Pressemitteilung des EDSB

EDSB: Aktive Aufsicht hält die EU-Einrichtungen beim Datenschutz auf dem richtigen Weg

Die EU-Einrichtungen befolgen die Datenschutzregeln und Prinzipien zum Schutz der Privatsphäre besser als je zuvor. Dies ist die Hauptaussage des am 24. Januar 2014 veröffentlichten Berichts des EDSB zu seiner jüngsten allgemeinen Vergleichserhebung.

Ich bin erfreut über die Fortschritte, die die EU-Einrichtungen gemacht haben. Zehn Jahre unserer aktiven Aufsicht haben zu einer deutlich besseren Regelbefolgung quer durch die EU-Einrichtungen geführt. Dies ist ein kraftvolles Signal dafür, dass die Einrichtungen verstanden haben, dass sie für die Anwendung der Datenschutzregeln rechenschaftspflichtig sind.

Peter Hustinx, EDSB

Bericht des EDSB

Pressemitteilung des EDSB

AUFSICHT

Menschlicher Fehler führt zu Sicherheitsverletzungen

Am 27. November 2013 wurde der EDSB auf einen offensichtlichen Verstoß gegen die Verordnung (EG) Nr. 45/2001 hingewiesen, bei dem es nach einem Einstellungsverfahren einer EU-Agentur zur Bekanntgabe der E-Mail-Adressen von Bewerbern gekommen war. Wie sich herausstellte, hatte ein Mitarbeiter der Personalabteilung eine E-Mail versandt, die 205 nicht ausgewählte Bewerber darüber informieren sollte, dass ihre Bewerbung auf eine bestimmte Stelle nicht erfolgreich war. In diesem besonderen Fall war dem Mitarbeiter des Personalteams ein manueller Fehler unterlaufen: Anstatt alle Adressen als Blindkopien im Feld „BCC" der E-Mail einzutragen, hatte er sie versehentlich in das Feld „AN" übernommen. Wir konnten uns überzeugen, dass die Agentur zum Zeitpunkt des Vorfalls angemessene Vorkehrungen getroffen hatte, um eine Gefährdung personenbezogener Daten zu minimieren. Nach dem Vorfall wurden (oder werden) verschiedene weitere Maßnahmen ergriffen, um das Risiko etwaiger anderweitiger Bekanntgabe zu verringern. Wir sind zu der Erkenntnis gekommen, dass diese konkrete Verletzung des Datenschutzes durch einen manuellen Fehler verursacht wurde, der nicht auf eine Nachlässigkeit der Agentur im Bereich der Datensicherheit zurückzuführen ist.

Konsultation des EDSB

Das neue Statut der EU-Beamten und die Weiterverarbeitung von Personalbeurteilungen

Das neue *Statut* der EU-Beamten sieht beim jährlichen Beurteilungsverfahren oder dem Laufbahnentwicklungsbericht einige Veränderungen vor. Im Statut heißt es, dass eine unzulängliche jährliche Beurteilung den Aufstieg in die nächste Dienstaltersstufe nach zwei Jahren blockiert, dass drei aufeinander folgende zu einer Zurückstufung und fünf aufeinander folgende zur Entlassung des Betroffenen führen.

Sobald die entsprechenden allgemeinen Durchführungsbestimmungen erlassen waren, hat der Datenschutzbeauftragte (*DSB*) der Kommission den EDSB über die erste Weiterverwendung des Laufbahnentwicklungsberichts informiert.

In unserem Schreiben vom 28. Januar 2014 haben wir darauf bestanden, dass Betroffene über den weiteren zusätzlichen Zweck der Verarbeitung der für die jährlichen Beurteilungen erhobenen Daten sowie über ihr Einspruchsrecht *unterrichtet* werden.

Da Artikel 110 des neuen Statuts vorsieht, dass die allgemeinen Durchführungsbestimmungen der Kommission grundsätzlich für alle 44 Agenturen gelten, hat der EDSB beschlossen, seine Empfehlungen in dieser Sache an alle DSB zu übermitteln, um die in dieser Angelegenheit notwendigen Leitlinien bereitzustellen.

Schreiben des EDSB

ARACHNE: Kein Spinnennetz für den Datenschutz

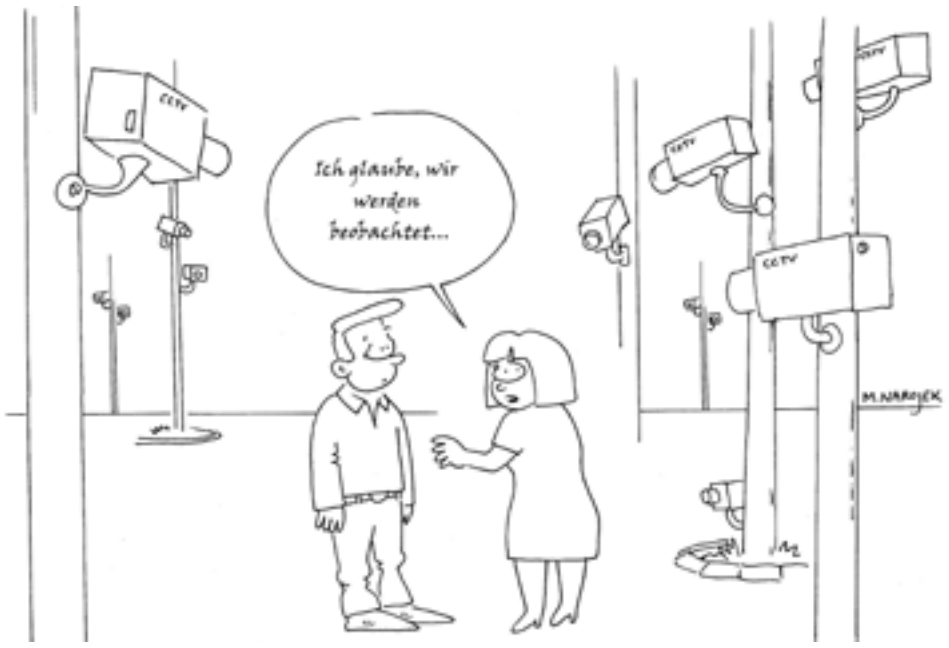
Das Risikoanalysesystem ARACHNE ist Teil der Strategie der Europäischen Kommission zur Verhütung und Aufdeckung von Betrug im Bereich der Strukturfonds (Europäischer Sozialfonds und Europäischer Fonds für regionale Entwicklung). Es ergänzt eine bestehende Datenbank mit öffentlich zugänglichen Informationen und soll auf Grundlage einer Reihe von Risikoindikatoren besonders riskante Projekte ermitteln; dadurch werden die Prüfer bei der Identifizierung und Auswahl künftiger Prüfungskandidaten unterstützt. Anders als andere, auf die Betrugserkennung ausgerichtete Verarbeitungsvorgänge versucht ARACHNE nicht, das individuelle Verhalten von Mittelempfängern zu beurteilen oder Begünstigte vom Mittelempfang auszuschließen.

Die Empfehlungen in unserer Stellungnahme vom 17. Februar 2014 verweisen u. a. auf die Notwendigkeit, die Datenqualität zu gewährleisten, und auf die Information der betroffenen Personen. Angesichts des Umstands, dass ARACHNE beispielsweise Informationen über sanktionierte Personen enthält, haben wir uns für die Einführung einer spezifischeren Rechtsgrundlage ausgesprochen, die zur Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Artikel 10 Absatz 5 der Verordnung befugt.

Stellungnahme des EDSB

Videoüberwachung: Der EDSB begrüßt Verbesserungen bei Einrichtungen der EU

Gestützt auf unsere Leitlinien zur Videoüberwachung aus dem Jahr 2010 und wie in unserem Kontrollbericht aus dem Jahr 2012 angekündigt, hat der EDSB 2012 gezielte Vor-Ort-Kontrollen bei 13 Organen und Einrichtungen mit Sitz in Brüssel und 2013 vier ähnliche Vor-Ort-Kontrollen in Luxemburg durchgeführt. Dabei ging es hauptsächlich um die Art und Weise, in der die allgemeine Öffentlichkeit über die Videoüberwachung informiert wird. Der Bericht über die Vor-Ort-Kontrollen in Luxemburg wurde am 13. Januar 2014 veröffentlicht. Nach der Verordnung (EG) Nr. 45/2001 sind EU-Organe und Einrichtungen rechenschaftspflichtig; mit anderen Worten, sie müssen ihren Verpflichtungen nachkommen und gegenüber der Kontrollbehörde, dem EDSB, nachweisen, dass sie dies getan haben. Die positiven Ergebnisse dieser neuesten Vor-Ort-Kontrollen zeigen, dass unsere Empfehlungen umgesetzt wurden - ein erfolgreiches Beispiel dafür, dass EU-Organe und Einrichtungen den Grundsatz der Rechenschaftspflicht zur Anwendung bringen.



Pressemitteilung des EDSB

Informationsblatt des EDSB zur Videoüberwachung

BERATUNG

Fortschritte beim Datenschutzreformpaket

Die vorgeschlagene Datenschutzgrundverordnung wird unter griechischem Ratsvorsitz weiterhin im Rat erörtert. In einem Schreiben an den Präsidenten des Rates der Europäischen Union vom 14. Februar haben wir unsere Auffassung zu **drei wesentlichen Aspekten** der Reform dargelegt, bei denen noch Klärungsbedarf besteht.

An erster Stelle haben wir betont, **dass der öffentliche Sektor auch weiterhin in den Geltungsbereich der Datenschutzgrundverordnung fallen muss**. Tatsächlich würde die Einführung einer weit gefassten Ausnahme, wie sie offensichtlich von einigen Mitgliedstaaten befürwortet wird, einen Rückschritt gegenüber dem derzeitigen Datenschutz-*Besitzstand* bedeuten, denn weder die Datenschutzrichtlinie 95/46/EG noch das Übereinkommen Nr. 108 des Europarats unterscheiden zwischen öffentlichem und privatem Sektor. Noch wichtiger ist, dass viele Maßnahmen etwa im Bereich der Gesundheitsversorgung von öffentlichen wie von privaten Stellen durchgeführt werden; für beide sollten dieselben Vorschriften gelten.

Auch bei der heftig diskutierten Frage der **zentralen Anlaufstelle** (one-stop-shop) haben wir uns eingebracht und auf die Bedeutung hingewiesen, die dieser Grundsatz für die vorgeschlagene Harmonisierung des Datenschutzrahmens hat. Nach unserer Auffassung werden die Rechte der betroffenen Personen auf wirksame Rechtsmittel und ein faires Verfahren durch den Grundsatz der zentralen Anlaufstelle nicht unangemessen eingeschränkt; tatsächlich ist er mit hohen Schutzstandards für die Grundrechte der Bürger vereinbar, darunter auch diejenigen, die durch Artikel 47 der Charta der Grundrechte geschützt sind.

Schließlich haben wir noch zum **Grundsatz der Rechenschaftspflicht** und zum „risikobasierten Ansatz" Stellung genommen und darauf hingewiesen, dass unbedingt klare Kriterien erforderlich sind, anhand derer Risikobewertungen durchgeführt werden, um die Einhaltungsbemühungen in Bereiche zu lenken, in denen sie besonders nötig sind.

Zahlungen im Binnenmarkt

Am 5. Dezember 2013 haben wir eine Stellungnahme zum Gesetzgebungspaket für *Zahlungsdienste im Binnenmarkt und Interbankentgelte für kartengebundene Zahlungsvorgänge* veröffentlicht. Die Richtlinie soll Verbrauchern verschiedene neue Rechte einräumen, während eine begleitende Verordnung die Gebühren deckelt, die Einzelhändler für die Bearbeitung von Debit- und Kreditkartenzahlungen an Banken zahlen müssen, und damit auch die Kosten der Verbraucher senken sollte. In unserer Stellungnahme begrüßen wir die Einführung einer materiellrechtlichen Vorschrift, nach der jede Verarbeitung personenbezogener Daten, die im Rahmen der vorgeschlagenen Richtlinie erfolgt, die nationalen Gesetze zur Umsetzung der Richtlinie 95/46/EG, der Richtlinie 2002/58/EG und der Verordnung (EG) Nr. 45/2001 in vollem Umfang achten muss.

Wir haben empfohlen, Verweise auf das anwendbare Datenschutzrecht mit konkreten Garantien zu formulieren, die für alle Situationen gelten, in denen die Verarbeitung personenbezogener Daten vorgesehen ist, und dass ausdrücklich klargestellt werden sollte, dass die Verarbeitung personenbezogener Daten nur in dem Umfang durchgeführt werden darf, der für die Abwicklung der Zahlungsdienste erforderlich ist. Wir haben auch noch auf andere Aspekte des Datenschutzes z. B. beim Informationsaustausch, beim Zugriff Dritter auf Kontoinformationen und bei Sicherheitsberichten hingewiesen.

Stellungnahme des EDSB

Unterbindung des illegalen Handels mit Schusswaffen muss Datenschutzziele berücksichtigen

In unserer Stellungnahme vom 17. Februar 2014 zur Mitteilung der Kommission über *Schusswaffen und die innere Sicherheit der EU: Schutz der Bürger und Unterbindung des illegalen Handels* haben wir auf die geltenden Datenschutzanforderungen, insbesondere für die in der Mitteilung beschriebenen Prioritäten und Aufgaben hingewiesen.

Wir haben nachdrücklich gefordert, dass diese Aspekte in einer frühen Phase des Gesetzgebungsverfahrens berücksichtigt werden (wenn möglich bei der Konsultation der Interessenträger), und dass in jeden Rechtstext ein Verweis auf das anzuwendende Datenschutzrecht aufzunehmen ist.

Im Einzelnen haben wir Fragen des Datenschutzes im Zusammenhang mit folgenden Aspekten angesprochen:

- Kennzeichnung von Schusswaffen,
- schließliche Einführung einer obligatorischen ärztlichen Untersuchung und einer Strafregisterüberprüfung als Voraussetzung für den rechtmäßigen Erwerb und Besitz einer Schusswaffe,
- Installation biometrischer Sensoren in Schusswaffen und
- Informationsaustausch zwischen Strafverfolgungs- und Zollbehörden, insbesondere über IT-Großsysteme.

Stellungnahme des EDSB

Datenabgleich zur Bekämpfung von grenzüberschreitendem Sozialversicherungsbetrug benötigt Datenschutzgarantien

Die Kommission ersuchte den EDSB um vorläufige Kommentare zu einem erwogenen Vorschlag zur Änderung der Verordnung zur *Koordinierung der Systeme der sozialen Sicherheit*, der die Verfahren zur Bekämpfung des grenzüberschreitenden Sozialversicherungsbetrugs verbessern soll – und zwar insbesondere beim Informationsaustausch zwischen Mitgliedstaaten.

Der Datenabgleich ist ein Verfahren, bei dem zwei Sätze von personenbezogenen Daten miteinander verglichen werden, um alle widersprüchlichen Informationen zu ermitteln. Beispielsweise liefert ein Mitgliedstaat Daten über Todesfälle an das Herkunftsland der Verstorbenen, die dieses dann anhand seiner eigenen Liste von Renten (oder anderen Bezügen), die an Staatsangehörige mit Wohnsitz in einem anderen Mitgliedstaat gezahlt werden, überprüfen kann.

In unseren Kommentaren vom 17. Januar 2014 haben wir die Absicht begrüßt, den derzeitigen Rechtsrahmen zu ändern, um mehr Klarheit beim Austausch großer Datenmengen in Form des „Datenabgleichs" zu schaffen. Dabei haben wir auf die Notwendigkeit und Verhältnismäßigkeit aller Datenabgleichverfahren gedrungen und darauf hingewiesen, dass es besonders wichtig ist,

- Transparenz über den Gegenstand des Datenabgleichs sicherzustellen,
- zu gewährleisten, dass gestützt auf Ergebnisse eines Datenabgleichs Leistungen nicht automatisch verweigert werden, und
- faire Verfahren für betroffene Personen zu garantieren, die auf automatische Abgleiche gestützte Entscheidungen anfechten möchten.

Kommentare des EDSB

Schutz personenbezogener Daten in der Nahrungsmittelkette

Derzeit wird eine neue Verordnung über *amtliche Kontrollen und andere amtliche Tätigkeiten zur Gewährleistung der Anwendung des Lebens- und Futtermittelrechts* im Europäischen Parlament und im Rat erörtert. Der Vorschlag sieht vor, dass zwei allgemeine Datensätze verarbeitet werden sollen, nämlich Daten über die Unternehmer (z. B. Namen von natürlichen Personen oder Unternehmen, Ort der Niederlassung, Websites, Einstufungen usw.) und Daten über Vermögensgegenstände der Unternehmer (z. B. Tiere und Waren). Außerdem beschreibt er den Informationsaustausch zwischen den zuständigen nationalen Stellen über ein EU-weites IT-Netzwerk, das sogenannte „IMSOC".

In unseren Kommentaren vom 20. Februar 2014 haben wir Folgendes klargestellt:

- Daten zu Waren und Tieren könnten solche *über* einen *bestimmten oder bestimmbaren* einzelnen Unternehmer sein und fallen deshalb unter den Begriff der „personenbezogenen Daten".
- Datenschutzvorschriften finden auf die in der Verordnung geplante Datenverarbeitung Anwendung, soweit es sich um Daten über einen Unternehmer handelt, der sein Geschäft als natürliche Person betreibt, oder soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt, oder sich Informationen über juristische Personen auch auf natürliche Personen „beziehen", oder wenn innerstaatliche Gesetze, einschließlich der Gesetze zur Umsetzung der Richtlinie 95/46/EG, den Schutz personenbezogener Daten auch auf juristische Personen ausdehnen.

Das IMSOC soll den Ansatz des eingebauten Datenschutzes und der datenschutzfreundlichen Voreinstellungen umsetzen, wobei die Kommission dafür verantwortlich sein soll, den Austausch personenbezogener Daten innerhalb des Systems zu kontrollieren; hierzu gehört, dass sie auf ihrer mehrsprachigen Website (auch „im Namen" zuständiger Behörden) für betroffene Personen eine erste „Schicht" von Datenschutzhinweisen und weitere einschlägige Informationen bereitstellt.

EDSB ,Kommentare

Internettechniker diskutieren über besseren Schutz der Privatsphäre und mehr Sicherheit

Die Internet Engineering Task Force (IETF) ist eine nicht gewinnorientierte Organisation, die Internetstandards und insbesondere die Internet-Protokollsuite (TCP/IP usw.) entwickelt und fördert. Beim IETF-Treffen, das Anfang März dieses Jahres in London stattfand, kamen die Internettechniker auf die Ergebnisse ihrer vorigen Sitzung (letzter November in Vancouver, siehe dazu auch unseren Bericht im *Newsletter* des EDSB vom Dezember 2013) zurück, in der sie beschlossen hatten, die massive Überwachung der Internetkommunikation als Bedrohung einzustufen und diese Bedrohung (wie andere auch) durch technische Maßnahmen abzuwehren. Teil des IETF-Treffens in London waren Workshops zur Privatsphäre und Diskussionen darüber, wie sich die Privatsphäre in der Grundstruktur des Internets über dessen Protokolle am besten verankern lässt. Dem IETF-Treffen vorangegangen war ein dedizierter *Workshop* mit mehr als 100 IT-Spezialisten, die mehr als 60 Beiträge zu Möglichkeiten diskutierten, wie sich das Internet gegen seine allgegenwärtige Überwachung wappnen lässt.

Höchste Priorität vieler Techniker ist die wirksame Nutzung richtig umgesetzter kryptografischer Instrumente (maschinennah programmierte Algorithmen, die häufig für den Aufbau von Computersicherheitssystemen eingesetzt werden), um die Sicherheit der Netze und der Kommunikation zu erhöhen. Experten für das Thema Privatsphäre haben bereits darauf hingewiesen, dass bei der technischen Auslegung auch andere Grundsätze der Privatsphäre wie Datenminimierung, Anonymisierung und Aggregation berücksichtigt werden sollten. Die Suche nach nützlichen technischen Lösungen, mit denen sich diese Grundsätze umsetzen lassen, ist eine Aufgabe, die auch weiterhin einer breiten Zusammenarbeit bedarf. Der EDSB schlägt eine *Initiative* vor, um die Kommunikationslücke zwischen Privatsphärenexperten und Technikern zu schließen; dann könnten sie gemeinsam an technischen Instrumenten arbeiten, mit denen sich die Privatsphäre in Internet-Tools und -Anwendungen besser schützen lässt. Internetentwickler werden um Interessenbekundungen gebeten.

Wird mobile Sicherheit zur entscheidenden Herausforderung für die Privatsphäre?

Funktionen der Mobilkommunikation werden zur Haupttriebkraft in der vernetzten Welt. Immer mehr Geräte sind mit Wi-Fi, Bluetooth, 4G oder anderen Schnittstellen ausgerüstet, die eine Verbindung mit dem Internet entweder direkt oder über Smartphones oder private Netze ermöglichen. Tragbare Geräte etwa zur Kontrolle sportlicher Leistungen mit Satellitennavigationsfunktionen erfassen biometrische Daten sowie den Standort und die Bewegung ihrer Nutzer und übertragen diese Daten zu den Servern ihrer Hersteller, sobald sie verbunden sind. Haushaltsgeräte können mit lokalen Netzen kommunizieren, und Kraftfahrzeuge können Daten zu ihren Funktionen, zu ihrer Position und zum Verhalten ihrer Fahrer erfassen und übertragen.

Internetgiganten investieren beträchtliche Summen in mobile und und eingebettete Technologien: Erst kürzlich wurden mehrere Firmen aus den Bereichen mobile Nachrichtendienste, Heimautomatisierung und Robotik übernommen. Außerdem investieren sie massiv in die Forschung und Entwicklung von Mobilität z. B. durch autonome Kraftfahrzeuge.

Während diese Trends wahrscheinlich dazu führen, dass mehr personenbezogene Daten gesammelt und über die Netze übertragen werden, bestehen Bedenken, dass die Sicherheit dabei nicht Schritt halten könnte. Auch die Anzahl gravierender Sicherheitslücken, die in weitverbreiteten Systemen entdeckt werden, nimmt zu. Ein kürzlich behobener *Programmierfehler* hatte dazu geführt, dass einige der populärsten Mobilgeräte für Man-in-the-Middle-Angriffe anfällig waren, sodass der Angreifer scheinbar verschlüsselte Kommunikationen abfangen konnte. Kurz nach diesem Vorfall wurde auch ein Problem mit quelloffener Software entdeckt. Ein Stück Programmcode, der in vielen Linux-Systemen vorkommt, hatte eine *kritische Schwachstelle*, die es Angreifern ermöglichte, bestimmte Sicherheitsvorkehrungen der Transport Layer Security (TLS) zu umgehen. Das bedeutet, dass Programme, die die betroffenen Pakete verwenden, durch Angriffe verwundbar sind, die eine Decodierung von verschlüsselter Kommunikation ermöglichen. In beiden Fällen sind seither Softwareupdates zur Behebung der Fehler bereitgestellt worden. Eine weitere Schwachstelle wurde kürzlich bei einem Smartphone mit dem Betriebssystem Android entdeckt; hier konnte der für die Netzkommunikation zuständige Chip alle Einschränkungen umgehen, die den „smarten" Bereich des Handys schützen, und so Zugriff auf alle im Smartphone gespeicherten Informationen erhalten. Wer immer die Kontrolle über das Kommunikationsmodul übernahm, konnte damit eine *Hintertür* in das Smartphone des Nutzers öffnen. Auch für diese spezielle Konfiguration ist eine Lösung entwickelt worden, die aber nicht alle betroffenen Smartphones schnell erreichen dürfte.

Während die Software der meisten Computer und vieler Mobilgeräte häufig aktualisiert wird, sodass Versionen installiert sind, die frei von bekannten Schwachstellen sind, ist dies bei anderen Geräten mit integrierten Kommunikationsfunktionen wie Fernseh- oder Haushaltsgeräten sehr viel weniger sicher. Bei solchen Geräten endet die Bereitstellung von Softwareupdates oft schon kurz nach ihrem Verkauf und lange vor Ablauf ihrer üblichen Nutzungsdauer. Schwachstellen ihrer „alten" Betriebssysteme und Funktionen bleiben erhalten und können Angreifern Zugang bieten, die sich dabei auf die wohl bekannten Schwachstellen älterer Softwareversionen stützen. Wie sich zeigte, besitzen selbst einige Router, die den Zugang zum Netz herstellen, solche Schwachstellen.

Diese Situation bedeutet für Hersteller, Händler und Diensteanbieter, die das Internet der Dinge oder das Internet aller Dinge aufbauen wollen, eine gewaltige Herausforderung. Geräte müssen so entwickelt werden, dass sie sicher sind und durch regelmäßige operative Aktualisierungen auch sicher bleiben können. Ohne eine Lösung dieses Problems könnten gerechtfertigte Sicherheitsbedenken die Verbreitung vernetzter Geräte erheblich behindern.

VERANSTALTUNGEN

Eröffnung des EDSB-Labors im Frühjahr

Um unsere technologischen Überwachungskapazitäten auszuweiten und die Datenschutzfunktionen bestimmter Produkte oder Systeme beurteilen zu können, die im Bereich unserer Aufsichtstätigkeit zum Einsatz kommen, hatte der EDSB 2013 Pläne zur Errichtung eines IT-Labors entwickelt. Das Labor soll uns bei der Bewertung der Auswirkungen helfen, die neue technische Entwicklungen bei Geräten für die Mobilkommunikation auf die Privatsphäre haben, und die Prüfung erleichtern, ob Websites die Datenschutzvorschriften einhalten. Das IT-Labor des EDSB wird seinen Betrieb im Frühjahr 2014 aufnehmen.

Das Labor kann auch dazu dienen, neue oder veränderte Plattformen zu prüfen, die für den Datenschutz wichtig sind; Beispiele sind Forschungsergebnisse von Universitäten oder neue Industrieprodukte.

In Zukunft können wir IT-Absolventen im Anschluss an unser Praktikumsprogramm oder Graduierten, die einen Teil ihrer Forschungszeit beim EDSB verbringen, die Nutzung der Laboreinrichtungen für Forschungs- und Entwicklungsprojekte anbieten. Mit Hilfe des Labors könnten sie Forschungs- und Entwicklungsarbeit im technischen Bereich leisten und Experimente durchführen.

Angesichtes dieser Möglichkeiten möchten wir aktiver für das *Praktikumsprogramm* des EDSB werben; Zielgruppen sind Studierende der Informatik und verwandter Fächer, die sich auch dafür interessieren, die technischen Aspekte des Datenschutzes und der Privatsphäre zu untersuchen. Der EDSB bietet Universitätsabsolventen ein bezahltes fünfmonatiges Praktikum und Graduierten, die bereits aus anderen Programmen unterstützt werden und besondere Forschungsaufgaben in Brüssel verfolgen möchten, die Option eines unbezahlten Praktikums.

BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

VORTRÄGE UND VERÖFFENTLICHUNGEN

- Vortrag (*pdf*) von Peter Hustinx in Brüssel, „Opportunities and challenges in the digital era: big data and moral hazard“ (1. April 2014)
- Vortrag (*pdf*) von Peter Hustinx in Brüssel, „Anmerkungen zur Datenschutzkontrolle bei Europol“ (12. Februar 2014)
- Vortrag (*pdf*) von Peter Hustinx in Bonn, „Amtswechsel: Verabschiedung und Amtseinführung“ (4. Februar 2014)
- Vortrag (*pdf*) von Peter Hustinx in Bonn, „Der EU-Binnenmarkt-Vorschlag für den elektronischen Kommunikationssektor als Spannungsfeld zwischen Datenschutz, Netzneutralität und wirtschaftlicher Freiheit“ (13. Januar 2014)

Über diesen Newsletter

Dieser Newsletter wird vom Europäischen Datenschutzbeauftragten herausgegeben – einer unabhängigen Behörde der EU, die im Jahr 2004 errichtet wurde und folgende Aufgaben hat:

- Überwachung der Verarbeitung personenbezogener Daten durch die EU-Verwaltung;
- Beratung zu Rechtsvorschriften im Bereich des Datenschutzes;
- Zusammenarbeit mit vergleichbaren Behörden, um einen kohärenten Datenschutz sicherzustellen.

Sie können diesen Newsletter über unsere Website abonnieren / abbestellen.

KONTAKT

www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
NewsletterEDPS@edps.europa.eu

POSTANSCHRIFT

EDSB
Rue Wiertz 60 – MTS Gebäude
B-1047 Brüssel
BELGIEN

DIENSTSTELLE

Rue Montoyer 30
B-1000 Brüssel
BELGIEN

Folgen Sie uns auf Twitter: @EU_EDPS

EDSB – Der europäische Hüter des Datenschutzes

QT-AC-14-001-DE-C