Betreff: WG: Unverschlüsselte Internetangebot "www.hh.hinweisportal.de"
Anlagen: 87_DSKMenschenrechteElektrischeKommunikation.pdf; AnlageEntschliessungElektronische Kommunikation.pdf

Wichtigkeit: Hoch

Von: [redacted]
Gesendet: Montag, 10. Juli 2017 10:06
An: [redacted]
Cc: [redacted]
Betreff: Unverschlüsselte Internetangebot "www.hh.hinweisportal.de"
Wichtigkeit: Hoch

Sehr geehrter [redacted],
sehr geehrter [redacted],

der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist auf das Hinweisportal der Polizei „http://hh.hinweisportal.de/~portal/de" aufmerksam gemacht worden und sieht diesbezüglich einen dringenden Handlungsbedarf, damit das informationelle Selbstbestimmungsrecht der Hinweisgeberinnen und –geber durch eine zumindest ausreichend ausgestaltete Datensicherheit gewährleistet ist.

Hierzu im Einzelnen:

Auf der Seite http://www.hamburg.de/g20-gipfel/8978178/hinweisportal/ gibt die Polizei Hamburg bekannt:

„Im Zusammenhang mit den im Rahmen der G20-Proteste in Hamburg begangenen Straftaten haben wir für Hinweise ab sofort die Internetseite hh.hinweisportal.de für den Upload von Fotos & Videos eingerichtet. Der Medienupload bietet selbsterklärend sehr vielfältige Möglichkeiten, der Polizei die Dateien zu Verfügung zu stellen."

Der Link führt dabei auf das **unverschlüsselte** Angebot http://hh.hinweisportal.de/, bei dem es sich offenbar um eine Unterseite eines vom BKA betriebenen Portals handelt. In dieser Form führt der Hinweis dazu, dass die Nutzer aufgefordert werden, auch sensible Daten über eine **ungesicherte** http-Verbindung zu versenden, obwohl das Portal auch per https://hh.hinweisportal.de/ und damit SSL-verschlüsselt erreichbar wäre.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits mit der Entschließung vom 27.03.2014, die ich Ihnen nebst dortiger Anlage vorsorglich beifüge, unter dem Titel „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" unter Ziffer 4 die Anforderung gestellt, dass Internetangebote in einer sicheren und vertrauenswürdigen Weise bereitgestellt werden müssen. Hierzu heißt es in den Ausführungen der Anlage zu Ziffer 4:

„Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden."

Rechtlicher Hintergrund der Pflicht auch der Polizei Hamburg, bei der Bereitstellung einer Möglichkeit zur elektronischen Kontaktaufnahme technische Maßnahmen insbesondere in Form einer hinreichenden Verschlüsselung zu ergreifen, ergibt sich aus § 8 Hamburgisches Datenschutzgesetz (HmbDSG). Hiernach ist jede Daten verarbeitende Stelle verpflichtet, u.a. die Vertraulichkeit und die Integrität bei der personenbezogenen Datenverarbeitung sicherzustellen. Durch eine hirneichende Verschlüsselung können die personenbezogenen Daten der Hinweisgeberinnen und –geber vor allem gegen deren Kenntnisnahme unbefugter Dritter geschützt werden.

Angesichts dieser gesetzlichen Bedingungen fordern wir Sie hiermit auf, zunächst umgehend folgende Maßnahmen zu ergreifen:

1. Das Hinweisportal der Polizei Hamburg muss in erster Linie in seiner verschlüsselten Variante aufgerufen werden können. Hierzu zählt insbesondere, dass eine Verlinkung ausschließlich auf https://hh.hinweisportal.de/ erfolgt.

2. Um jegliche Gefahr der Übertragung personenbezogener Daten ohne die erforderlichen Schutzmaßnahmen zu vermeiden, sollte das Angebot hh.hinweisportal.de überhaupt nur mittels SSL-Verschlüsselung aufrufbar sein, z.B. indem bei Aufruf von http://hh.hinweisportal.de/ automatisch auf https://hh.hinweisportal.de/ weitergeleitet wird.

3. Soweit für technische Maßnahmen im Zusammenhang mit dem Hinweisportal das BKA zuständig sein sollte, muss dieses umgehend entsprechend den Ziffern 1 und 2 durch die Polizei Hamburg aufgefordert werden.

Da es bereits zu einer enormen Nutzungshäufigkeit des Hinweisportals der Hamburger Polizei gekommen ist und eine intensive weitere Nutzung zu erwarten ist, bitten wir Sie hiermit, uns noch heute bis 16 Uhr eine schriftliche Stellungnahme insbesondere zu den Aufforderungen zukommen zu lassen, in der Sie uns über die durch die Polizei ergriffenen Maßnahmen informieren.

Da es sich nach unserem Kenntnisstand bei dem Angebot „hinweisportal" um eine Plattform des BKA handelt, bitten wir zugleich um Mitteilung, ob die eingehenden Daten nicht nur der Polizei Hamburg, sondern auch bzw. zunächst dem BKA zugehen.

Mit freundlichen Grüßen

[redacted]

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6, 20095 Hamburg
Telefon: 040/42854-4062 (Durchwahl) -4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: [redacted]

87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 27. und 28. März in Hamburg

Entschließung

Stand: 27. März 2014

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation"

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o.g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 27. und 28. März in Hamburg

Anlage zur Entschließung

Stand: 27.3.2014

„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation"

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten
   Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographische Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur
   Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.
   Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung
   Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.
   Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten
   Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten
   Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation
   Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen,
   Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird. Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung
   Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen.

Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können.
Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

- alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,
- für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,
- eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
- die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken.
Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen.
Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. <u>Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik</u>
Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.
Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. <u>Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung</u>
Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte

ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.
Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik
Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit
Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.