

ANTWORT

zu der

Anfrage des Abgeordneten Michael Hilberer (PIRATEN)

betr.: Zusammenarbeit des Bundesamtes für Sicherheit in der Informationstechnik mit ausländischen Diensten und deren Auswirkung

Vorbemerkung des Fragestellers:

„In seiner 30. Ausgabe vom 22.07.2013 weist der Spiegel dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die Rolle eines "Schlüsselpartners" der NSA zu. Dieses Amt spiele eine zentrale Rolle im Austausch der Dienste, auch auf internationaler Ebene. Aus diversen Geheimunterlagen ginge hervor, dass gesetzliche Rahmenbedingungen so geändert wurden, dass geschützte Daten deutscher Bürger und Firmen leichter an ausländische Partner herausgegeben werden können und das BSI diese gesetzlichen Änderungen durch seine sicherheitstechnischen Bewertungen zumindest gefördert habe. Obwohl sich das BSI als treuer Helfer von Bürgern, Unternehmen und staatlichen Institutionen bei IT-Sicherheitsproblemen aller Art ausgibt und das Monopol bei der Zertifizierung neuer IT-Produkte besitzt, würde die Behörde durch eine gezielte Aufweichung des grundrechtlich garantierten Schutz der digitalen Kommunikation und des ihr dienenden Datensicherheitsstandards das Speichern von Daten ausländischer Geheimdienste erleichtern und fördern, statt das Sicherheitsniveau für Bürger und Unternehmen zu verbessern. So nennt das BSI beispielsweise die DeMail "eine Infrastruktur für sichere Kommunikation" und zertifiziert diese, obwohl aus fadenscheinigen Gründen De-Mails auf dem Server des Anbieters kurz entschlüsselt und anschließend wieder verschlüsselt werden.

Kritiker mahnen, dass dadurch eine Schwachstelle entsteht, die sich Angreifer zunutze machen können - vergleichbar mit einem versiegelten Brief, der kurz geöffnet und anschließend wieder neu kuvertiert und versiegelt werde. Trotz dieser Sicherheitslücken wurde die De-Mail per Gesetz zu einem zuverlässigen Mittel, welches eine vertrauliche Kommunikation zwischen Sender und Empfänger gewährleiste.“

Vorbemerkung der Landesregierung:

Am 26.07.2013 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) u.a. zu der Berichterstattung des Spiegels folgende Stellungnahme veröffentlicht:

Im Rahmen der Medienberichterstattung zu den Ausspähprogrammen amerikanischer und britischer Geheimdienste ist auch über das Bundesamt für Sicherheit in der Informationstechnik (BSI) und dessen vermeintlich enge Zusammenarbeit mit dem US-Nachrichtendienst National Security Agency (NSA) berichtet worden. Dabei wurde unter anderem suggeriert, dass das BSI die NSA aktiv mit Informationen versorgt, die es der NSA erleichtern, in Deutschland Ausspähungen vorzunehmen und vorhandene Sicherheitsschranken zu umgehen. Hier wurde insbesondere eine vermeintliche Zusammenarbeit zwischen BSI und ausländischen Diensten im Zusammenhang mit der Zertifizierung von IT-Produkten und -Dienstleistungen – einer Kernaufgabe des BSI zur Schaffung von mehr IT-Sicherheit – unterstellt. Zudem wurde die Frage aufgeworfen, ob das BSI die NSA dabei unterstützt habe, Kommunikationsvorgänge am Internetknoten De-CIX auszuspähen.

Hierzu erklärt das BSI: Eine Zusammenarbeit oder Unterstützung ausländischer Nachrichtendienste durch das Bundesamt für Sicherheit in der Informationstechnik im Zusammenhang mit den Ausspähprogrammen Prism und Tempora findet nicht statt. Das BSI hat weder die NSA noch andere ausländische Nachrichtendienste dabei unterstützt, Kommunikationsvorgänge oder sonstige Informationen am Internet-Knoten De-CIX oder an anderen Stellen in Deutschland auszuspähen. Das BSI verfügt zudem nicht über das Programm XKeyscore und setzt dieses nicht ein. Das BSI gibt überdies keinerlei Informationen über zertifizierte IT-Produkte und -Dienstleistungen oder im Rahmen des Zertifizierungsprozesses gewonnene Erkenntnisse über diese Produkte und Dienstleistungen an andere Behörden, Nachrichtendienste oder sonstige Dritte weiter.

Das BSI tauscht sich im Rahmen seiner auf Prävention ausgerichteten Aufgaben regelmäßig mit anderen Behörden in der EU und außerhalb der EU zu technischen Fragestellungen der IT- und Internet-Sicherheit aus. Auch Behörden in Deutschland stellt das BSI auf Anfrage technische Expertise und Beratung zur Verfügung. Im Kontext der Bündnispartnerschaft NATO arbeitet das BSI auch mit der NSA zusammen. Diese Zusammenarbeit umfasst jedoch ausschließlich präventive Aspekte der IT- und Cyber-Sicherheit entsprechend den Aufgaben und Befugnissen des BSI gemäß des BSI-Gesetzes.

In Deutschland besteht eine strukturelle und organisatorische Aufteilung in Behörden mit einerseits nachrichtendienstlichem bzw. polizeilichem Auftrag und dem BSI mit dem Auftrag zur Förderung der Informations- und Cyber-Sicherheit. In anderen westlichen Demokratien bestehen mitunter Aufstellungen, in denen diese Aufgaben und Befugnisse in anderem Zuschnitt zusammengefasst werden. Die Zusammenarbeit des BSI mit diesen Behörden findet stets im Rahmen der präventiven Aufgabenwahrnehmung des BSI statt, unter anderem zur Abwehr von IT- und Cyber-Angriffen.

Unabdingbare Voraussetzung für die Nutzung von IT und das Erschließen der damit verbundenen wirtschaftlichen und gesellschaftlichen Potenziale ist das Vertrauen in die Informationstechnik und die IT-Dienstleistungen. Vertrauen setzt wiederum Sicherheit voraus, die das BSI zum Beispiel durch eine transparente und nachvollziehbare Darstellung der Sicherheitsanforderungen, der daraus resultierenden Sicherheitsniveaus und der Abläufe, wie Sicherheitsanforderungen entstehen, anstrebt. Die Zertifizierung ist ein bewährtes Verfahren zur Bewertung der Sicherheit von IT-Produkten, das international erfolgreich etabliert ist.

Die Objektivität und Einheitlichkeit der Prüfungen sowie die Unparteilichkeit wird dabei durch das BSI gewährleistet. Das BSI ist im Zertifizierungsverfahren maßgeblich an der Erarbeitung der Sicherheitsvorgaben (Security Targets) beteiligt. Nach der Beantragung der Zertifizierung beim BSI wird die technische Evaluierung eines Produktes im Regelfall durch eine beim BSI anerkannte private Prüfstelle durchgeführt, die der Antragsteller frei wählen kann. Die Prüfstelle wird vom Antragsteller beauftragt und bezahlt. Das BSI begleitet das Prüfverfahren und erteilt nach dessen erfolgreichem Verlauf und entsprechender Prüfung das Zertifikat.

Anbieter von IT-Produkten und -Dienstleistungen können mit Hilfe der Zertifizierung das Sicherheitsniveau ihrer Angebote nachvollziehbar darstellen. Nutzer von zertifizierten IT-Produkten und -Lösungen können einschätzen, für welche Einsatzbereiche diese Produkte und Dienstleistungen geeignet sind und welchen Beitrag die Nutzer ggf. selbst leisten müssen, um beim Einsatz dieser Produkte und Lösungen das erforderliche Maß an Informationssicherheit zu erreichen. Weitere Informationen zur Zertifizierung sind auf der Webseite des BSI abrufbar. Das BSI stellt allen gesellschaftlichen Gruppen in Deutschland Informationen zur Förderung der IT- und Cyber-Sicherheit zur Verfügung. Privatanwender erhalten Informationen auf den Internetseiten BSI-für-Bürger und können kostenlos den E-Mail-Newsletter Bürger-CERT abonnieren.

Dieser Stellungnahme ist aus Sicht der saarländischen Landesregierung nichts hinzuzufügen.

Im Rahmen der Umsetzung welcher Projekte, Anträge oder Gesetzentwürfe hat die Landesregierung auf die sicherheitstechnische Bewertung, Expertenwissen oder Gutachten des Bundesamts für Sicherheit in der Informationstechnik (BSI) vertraut? (Bitte nach jeweiligem Projekt, Antrag oder Gesetzentwurf und entsprechender Beratungstätigkeit des BSI einzeln aufschlüsseln).

Zu Frage 1:

Die Nutzung der vom BSI herausgegebenen IT-Grundschutz-Kataloge ist aufgrund der Vorschrift der saarländischen IT-Sicherheitsrichtlinie in allen Fragen der Datensicherheit verbindlich anzuwenden. Diese Vorgabe entspricht auch den Anforderungen des Unabhängigen Datenschutzzentrum Saarland und den Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik (IuK-Mindestanforderungen 2011).

Im Rahmen des bundesweiten Projektes zum Aufbau und Betrieb eines digitalen Sprach- und Datenfunknetzes der Behörden und Organisationen mit Sicherheitsaufgaben (Digitalfunk BOS) ist das BSI in unterschiedlichen Einzelprojekten (z. B. Ende-zu-Ende-Verschlüsselung, Standortdatenbank NetSite) eingebunden. Obwohl es sich nicht um ein ausschließlich saarländisches Projekt handelt, wird es hier benannt, da die in Länder- und Gemeindehoheit tätigen BOS mit ihrem wichtigsten Kommunikationsmedium betroffen sind.

Das BSI wird eingeschaltet, um die Vermessung im sog. Zonenmodell zur Bewertung von notwendigen Maßnahmen zum Schutz von Geräten gegen Abstrahlung durchzuführen, die beim Einsatz von Verschlüsselungsgeräten für den Verschlusssachengrad „Vertraulich“ und höher beachtet werden muss.

Die Polizei von Bund und Ländern vertraut im Rahmen der Organisation ihrer IT-Sicherheit regelmäßig auf sicherheitstechnische Bewertungen und Expertenwissen des BSI.

Die Vollzugspolizei des Saarlandes ist mit Ihrem IT-Sicherheitsbeauftragten in der Kommission IuK-Sicherheit des Unterausschusses IuK (Polizeiliche Informations- und Kommunikationsstrategie und -technik) des Arbeitskreises II (AK II) der Innenministerkonferenz (IMK) vertreten. In diesen Gremien werden Fragen der IT-Sicherheit für die Teilnehmer am polizeilichen Informationsverbund diskutiert und verbindlich geregelt.

Das BSI nimmt an den Sitzungen der Kommission IuK-Sicherheit grundsätzlich beratend teil.

Im Übrigen gibt es keine gemeinsame Projektarbeit saarländischer Landesdienststelle mit dem BSI oder eine direkte Beratung in Projekten. Eine enge Kommunikation besteht in Einzelfällen bei akut bestehenden Sicherheitsproblemen (z.B. entdeckte Sicherheitslücken in Standardsoftware).

Vertritt die Landesregierung die Auffassung, dass auch zukünftig auf die Expertise des BSI bei der Bewertung der Sicherheit informationstechnischer Projekte und Instrumente zurückgegriffen werden kann?

- a) Wenn ja, mit welcher Begründung vertraut die Landesregierung auch weiterhin dem BSI, das eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft sein soll, bei Problemstellungen in der Informationstechnik?
- b) Wenn nein, auf welche anderen Behörden oder externen Berater soll zukünftig bei der Bewertung von IT - Sicherheit zurückgegriffen werden?

Zu Frage 2:

Auf die Vorbemerkung wird verwiesen.

Welche Behörden oder externen Dienstleister neben dem BSI beraten die Landesregierung in Fragen der IT-Sicherheit? Bitte jeweils nach IT-Bereich, Themengebiet und beratendem Dienstleister / beratender Behörde einzeln aufschlüsseln.

Zu Frage 3:

Eine Beratung durch Behörden erfolgt projektübergreifend durch den Arbeitskreis IT-Sicherheit des Arbeitskreises der Datenzentralen der öffentlichen Verwaltung (ALD) und das Unabhängige Datenschutzzentrum Saarland.

Im Rahmen der beabsichtigten ISO 27001-Zertifizierung auf Basis von IT-Grundschutz wurden gemeinsam mit der Stadt Saarbrücken auf die diesbezüglichen Erfahrungen des Kommunalen Rechenzentrum Minden-Ravensburg/Lippe zurückgegriffen.

Zur Beratung wurden externe Dienstleister in folgenden Bereichen eingebunden: IT-Systeme der Zahlstelle im Bereich der Fördermaßnahmen Landwirtschaft - (InVeKos), IT-Systeme im Bereich der Fördermaßnahmen ESF und EFRE, Beratung im Rechenzentrumsbetrieb der ZDV-Saar, u.a. beim gezielten und gesteuerten Versuch die Sicherheitsarchitektur zu umgehen (Penetrationstests), Analyse- und Zertifizierungsprojekt zur umweltgerechten Modernisierung der IT der Landesregierung im Rechenzentrum als Grundlage zur Erfüllung des European Code of Conduct for Data Centres Energy Efficiency, Einbruch- und Brandmeldeanlagen im Rechenzentrum bei der ZDV-Saar sowie Beratung im Berechtigungsmanagement.

Eine Nennung der jeweils beauftragten Firmen soll aus Sicherheitsgründen an dieser Stelle nicht erfolgen, da daraus Rückschlüsse auf eingesetzte Sicherheitsarchitekturen gezogen werden könnten. Die Landesregierung bietet an, darüber im zuständigen Landtagsausschuss zu berichten.

Das BSI entwickelt sowohl Kodierungen der deutschen Auslandsvertretungen als auch die Software, die beim BND und Verfassungsschutz Anwendung findet. Darüber hinaus werden dort neue Telekommunikationsmittel untersucht und bewertet und Verschlüsselungssysteme geschaffen oder entschlüsselt. Inwiefern greift die Landesregierung auf vom BSI positiv bewertete Telekommunikationsmittel oder von diesem erstellte Verschlüsselungssysteme zurück?

Bitte nach Telekommunikationsmittel, Verschlüsselungssystem und Verwendungszweck einzeln aufschlüsseln.

Zu Frage 4:

Die Verschlüsselungssoftware „Chiasmus für Windows“ des BSI wird in verschiedenen Ressorts eingesetzt. Bei Übermittlungsdiensten im ISDN (Sprache, Telefax) kommt als Verschlüsselungsgerät Elcrodut 6-2 zum Einsatz. Im Bereich der Kommunikation im Digitalfunk sind die Funkgeräte mit BOS-Sicherheitskarten ausgestattet.

Des Weiteren werden sog. SINA-Boxen zur sicheren verschlüsselten Datenübertragung verwendet. Bei der sog. Virtuellen Poststelle erfolgt die Übertragung über das Internet mittels Ende-zu-Ende-Verschlüsselung auf Basis OSCI. Mobile Zugänge von Laptops / Notebooks werden über CISCO VPN-Tunnel gesichert.

Welche Voraussetzungen müssen innerhalb der Landesverwaltung erfüllt sein, um den Sicherheitsempfehlungen des BSI zu genügen?

Zu Frage 5:

Zur Umsetzung der Sicherheitsempfehlungen des BSI müssen personelle, technische, organisatorische und finanzielle Voraussetzungen in notwendigem Maße zur Verfügung stehen und werden im Rahmen der Projektplanung berücksichtigt.

Wird die Sicherheit des Landesdatennetzes bzw. die Datensicherheit des Datenverarbeitungszentrums des Saarlandes in regelmäßigen Abständen durch das BSI oder andere Behörden und externe Gutachter überprüft? Wenn ja, in welchen Intervallen findet eine solche Überprüfung statt und welche Kriterien werden hierbei sicherheitstechnisch bewertet?

Zu Frage 6:

Zurzeit erfolgen im Datenverarbeitungszentrum des Saarlandes Penetrationstests unter Beteiligung mehrerer Beratungsfirmen. Hier wird auf Frage 3 verwiesen. Desweiteren werden regelmäßige Audits nach Maßgaben der Europäischen Union (Fördermaßnahmen EFRE und ESF) durchgeführt. Das BSI ist an diesen Maßnahmen nicht unmittelbar und direkt beteiligt.

Wie hoch sind die personellen und finanziellen Mittel, die jährlich aufgewandt werden, um in der IT der Ministerien und der Staatskanzlei einer allgemeinverbindlichen Sicherheitsrichtlinie, die sich am BSI-Standard orientiert, gerecht zu werden?

Zu Frage 7:

Die Sicherheitsanforderungen an bestimmte Verfahren und Systeme sind in erster Linie Anforderungen, die sowohl der Verfügbarkeit, einer sachgerechten Aufgabenwahrnehmung als auch gleichzeitig der IT-Sicherheit dienen. Dies lässt eine separate Betrachtung und Berechnung der Aufwände als IT-Sicherheitsaufwände in der Regel nicht zu. Eine diesbezügliche Aufschlüsselung kann deshalb hier nicht erfolgen.

Verwenden die Landesregierung oder Behörden im Saarland vom BSI zertifizierte Kommunikationssysteme?

- a) Falls ja, wie bewertet die Landesregierung deren Sicherheit aufgrund der neuen Erkenntnisse der Zusammenarbeit von BSI und ausländischen Diensten?
- b) Falls nein, nach welchen Standards führt die Landesregierung derzeit sichere Kommunikation durch?

Zu Frage 8:

Auf die Antworten zu Frage 4 wird verwiesen.