

Kleine Anfrage

der Abgeordneten Jens Guth, Martin Haller, Margit Mohr und Carsten Pörksen (SPD)

und

Antwort

des Ministeriums des Innern, für Sport und Infrastruktur

Ausspähung privater Daten und Wirtschaftsspionage

Die **Kleine Anfrage 1895** vom 19. September 2013 hat folgenden Wortlaut:

Die aktuelle Diskussion um Ausspähungen von privaten Daten und mögliche Wirtschaftsspionage durch amerikanische und britische Geheimdienste verdeutlicht die Gefährdung von Gesellschaft und Wirtschaft. Das informationelle Selbstbestimmungsrecht tausender Bürgerinnen und Bürger wurde anscheinend verletzt. Nach Schätzungen entsteht der deutschen Wirtschaft durch (elektronische) Wirtschaftsspionage ein Gesamtschaden von bis zu 60 Milliarden Euro.

Vor diesem Hintergrund fragen wir die Landesregierung:

1. Wie schätzt die Landesregierung die Gefahr und die Auswirkungen dieses Skandals für Rheinland-Pfalz ein?
2. Hat die Landesregierung Erkenntnisse darüber, welche fremden Geheimdienste private Daten von rheinland-pfälzischen Bürgerinnen und Bürgern ausspähen und (elektronische) Wirtschaftsspionage bei rheinland-pfälzischen Firmen betreiben?
3. Gibt es Maßnahmen bzw. sind Maßnahmen seitens der Landesregierung geplant, um die rheinland-pfälzische Gesellschaft und Wirtschaft für das Thema zu sensibilisieren?
4. Wie bewertet die Landesregierung den Acht-Punkte-Maßnahmenkatalog des Bundesinnenministeriums und des Bundeswirtschaftsministeriums vom 14. August 2013 sowie das Zehn-Punkte-Programm des Bundeswirtschaftsministeriums vom 1. August 2013 mit seinen Empfehlungen für einen sicheren Umgang mit Unternehmensdaten im Internet?

Das **Ministerium des Innern, für Sport und Infrastruktur** hat die Kleine Anfrage namens der Landesregierung mit Schreiben vom 8. Oktober 2013 wie folgt beantwortet:

Zu Frage 1:

Die Nutzung des Internets hat gerade in den letzten Jahren einen rasanten Anstieg erlebt. Nach einer Studie der Initiative D21 sind etwa 78 Prozent der Rheinland-Pfälzer online. Damit liegt Rheinland-Pfalz an dritter Stelle der Flächenländer. Auch die Unternehmen tragen dieser Entwicklung Rechnung und stellen ihren Mitarbeitern zunehmend internetfähige Endgeräte zur Verfügung. Damit ist ein Zugriff auf firmeneigene Anwendungen von nahezu jedem Punkt der Welt aus möglich. Mit der Zunahme der Internetnutzung durch Bürger und Wirtschaft steigt selbstverständlich auch die Gefahr von Angriffen aus dem sog. Cyberspace. Deshalb wird es zunehmend wichtiger, gegen solche Attacken Vorsorgemaßnahmen zu ergreifen.

Nach wie vor liegen legal, aber auch illegal erworbene Informationen aus Wirtschaft, Forschung und Wissenschaft, Technik sowie Rüstung im Interesse einzelner Nachrichtendienste, aber auch von Konkurrenzunternehmen.

Die Landesregierung geht dieses Thema aktiv an, beispielsweise auf dem Mittelstandstag des Wirtschaftsministeriums im April 2013, auf dem gemeinsam mit dem rheinland-pfälzischen Verfassungsschutz der Wirtschaft die Bedrohung, aber auch mögliche Gegenmaßnahmen in den Unternehmen dargelegt wurden. Auch der dem Landtag vorgelegte Mittelstandsreport 2012 des Wirtschaftsministeriums geht auf dieses Thema ausdrücklich ein.

Je nach staatlicher Gesetzeslage, oder genauer gesagt in einigen Ländern ohne einschränkende Rechtsvorschriften, können deren Nachrichtendienste auch verdeckte Methoden zur Informationsbeschaffung im Internet nutzen. Bei solchen Maßnahmen kann auch ein gezielter Einbruch in das jeweilige Computersystem mit einem anschließenden Datenabfluss erfolgen.

b. w.

Das rlp-Netz, das gemeinsame Datennetz der Landesverwaltung und des Landtags, ist regelmäßig Ziel von Cyberangriffen. Im Schnitt werden täglich zwei bis fünf schwerwiegende Angriffe festgestellt, die sich teilweise bis nach China zurückverfolgen lassen. Anhaltspunkte dafür, dass diese Angriffe – die aufgrund unserer hohen Sicherheitsstandards bisher stets erfolglos waren – auf Maßnahmen westlicher Geheimdienste zurückgehen, bestehen nicht.

Dem rheinland-pfälzischen Verfassungsschutz liegen auch keine sonstigen belastbaren Erkenntnisse zu Spionageaktivitäten westlicher Nachrichtendienste gegen die Belange des Landes Rheinland-Pfalz vor. Bezüglich der Betroffenheit rheinland-pfälzischer Bürgerinnen und Bürger liegen keine Erkenntnisse vor. Dies gilt auch vor dem Hintergrund der Aussagen des „Whistleblowers“ Edward Snowden. Es bleibt abzuwarten, inwieweit die Anschuldigungen hauptsächlich gegenüber den USA letztlich verifiziert werden können.

Zu den Fragen 2 und 3:

Die Wirtschaft zählt seit jeher zu den klassischen Angriffszielen fremder Nachrichtendienste. Insbesondere die Russische Föderation und die Volksrepublik China betreiben intensive Wirtschaftsspionage in der Bundesrepublik. Im Fokus stehen Schlüsseltechnologien wie Umwelttechnologien, die elektronische und chemische Industrie sowie der Maschinen- und Anlagenbau. Mit einer Exportquote von über 50 Prozent nimmt Rheinland-Pfalz bundesweit eine Spitzenstellung ein. Eine erfolgreiche Abwehr von Wirtschaftsspionage ist daher für rheinland-pfälzische Unternehmen von existenzieller Bedeutung.

Mit der bereits Mitte der 90er Jahre gegründeten und in den letzten Jahren inhaltlich und organisatorisch breiter angelegten Sicherheitspartnerschaft nimmt Rheinland-Pfalz bundesweit eine Vorreiterrolle für die Einbindung von Wirtschaft, Wissenschaft und Forschung in präventive Abwehrstrategien ein. Durch gezielte Sensibilisierungsgespräche hat der Verfassungsschutz seine Präventionsarbeit auf hohem Niveau fortgesetzt. Nachgefragt wurden insbesondere Vortragsveranstaltungen in Unternehmerkreisen, Workshops und Tagungen, die durch ihre Multiplikatorenwirkung die Sensibilität für Spionagegefahren erhöhen sollen. Die von Internetattacken betroffenen Unternehmen stehen in Kontakt mit dem Verfassungsschutz und werden fortlaufend betreut. Ein ungewollter Informationsabfluss wurde allerdings bisher in Rheinland-Pfalz nicht bekannt.

Zur Absicherung der Daten, die Bürgerinnen und Bürger der Verwaltung im Rahmen von E-Government überlassen, verfolgt die Landesregierung eine ganzheitliche Informationssicherheitsstrategie. Diese setzt zum einen auf die Absicherung der zentralen IT-Infrastrukturen und zum anderen auf den zentralen Betrieb von geschäftskritischen Verfahren beim Landesbetrieb Daten und Information (LDI). Von besonderer Bedeutung ist hierbei das flächendeckende, hochsichere und hochverfügbare rlp-Netz. Noch vor Bekanntwerden der aktuellen Veröffentlichungen um „Tempora“ und „Prism“ wurde erkannt, wie wichtig eine eingehende Überprüfung der Konzepte für Schutz und Sicherheit der Daten durch externe Gutachter und Auditoren ist. Die gesamte technische Umsetzung und der Betrieb des rlp-Netzes wurden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen einer Zertifizierung untersucht. Im April dieses Jahres wurde durch das BSI das sogenannte ISO 27001-Zertifikat auf der Basis von IT-Grundschutz erteilt. Damit bestätigen die Gutachter, dass die IT-Basisinfrastruktur in Rheinland-Pfalz, das rlp-Netz, eine sichere Basis für die Verarbeitung und Speicherung der Daten der rheinland-pfälzischen Bürgerinnen und Bürger zur Verfügung stellt. Rheinland-Pfalz ist erst das zweite deutsche Bundesland, das diesen Nachweis erbringen konnte.

Zu Frage 4:

Das Acht-Punkte-Programm der Bundeskanzlerin zum besseren Schutz der Privatsphäre und der Fortschrittsbericht des Bundesinnenministeriums sowie des Bundeswirtschaftsministeriums und auch die 10 Punkte für den sicheren Umgang mit Unternehmensdaten im Internet sind ein erster Ansatzpunkt, aber aus Sicht der Landesregierung noch unzureichend. Bevor nicht klar ist, in welchem Umfang deutsche Grundrechtsträger ausgespäht werden, können diese Maßnahmen weder Bürgerinnen und Bürger noch Unternehmen wirksam schützen.

Aus diesem Grund muss die Spähaffäre vollständig aufgeklärt und das Thema Wirtschaftsspionage verstärkt in den Fokus genommen werden. Dies wird von der Bundesregierung nicht mit dem nötigen Nachdruck betrieben. Ministerpräsidentin Malu Dreyer fordert daher ein zeitnahes Spitzengespräch mit der Bundeskanzlerin, Vertretern der Länder und den Datenschutzbeauftragten. Die Bundesregierung muss in eine tiefe inhaltliche Auseinandersetzung mit dem Thema gehen und alles dafür tun, die Grundrechte der Bürgerinnen und Bürger auch vor Angriffen aus dem Ausland zu schützen. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern unterstützt diese Initiative von Ministerpräsidentin Dreyer.

In Vertretung:
Jürgen Häfner
Staatssekretär