LANDTAG RHEINLAND-PFALZ
16. Wahlperiode

Drucksache 16/5350
23. 07. 2015

Kleine Anfrage

der Abgeordneten Pia Schellhammer und Nils Wiechmann (BÜNDNIS 90/DIE GRÜNEN)

und

Antwort

des Ministeriums des Innern, für Sport und Infrastruktur

Hackerangriff auf rheinland-pfälzische Kfz-Zulassungsstellen

Die **Kleine Anfrage 3510** vom 3. Juli 2015 hat folgenden Wortlaut:

Am Montag, 22. Juni 2015, hat ein Hackerangriff auf Kfz-Zulassungsstellen in Rheinland-Pfalz und Hessen deren Schließung verursacht. Betroffen waren 39 rheinland-pfälzische Zulassungsstellen. In den letzten Tagen und Wochen wurde außerdem ein schwerwiegender Angriff auf das Datennetz des Deutschen Bundestags bekannt.
Vor diesem Hintergrund fragen wir die Landesregierung:
1. Welche Informationen hat die Landesregierung über den Hackerangriff auf die rheinland-pfälzischen Zulassungsstellen?
2. Welcher Schaden wurde durch den Angriff verursacht?
3. Wie sind rheinland-pfälzische Behörden gegen Hackerangriffe gesichert?
4. Welche Gefahren gehen allgemein durch Hackerangriffe aus?

Das **Ministerium des Innern, für Sport und Infrastruktur** hat die Kleine Anfrage namens der Landesregierung insbesondere auf der Grundlage von Informationen des Landesbetriebs Daten und Information (LDI) mit Schreiben vom 20. Juli 2015 wie folgt beantwortet:

Zu Frage 1:

Die Aufgaben der unteren Verwaltungsbehörde nach der Straßenverkehrs-Zulassungs-Ordnung werden von den Kreisverwaltungen, in kreisfreien und großen kreisangehörigen Städten von den Stadtverwaltungen wahrgenommen. Im Auftrag dieser kommunalen Zulassungsbehörden und in Abstimmung mit der Gesellschaft für Kommunikation und Wissenstransfer mbH (KommWIS) – sie trägt die fachliche Verfahrensverantwortung – betreibt der LDI das zentrale kommunale Verfahren zur Kraftfahrzeug-Zulassung. Teilkomponente jenes Verfahrens ist ein aus dem Internet erreichbares Web-Portal zur Reservierung von Kfz-Wunschkennzeichen (KFZ-WKZ).

Im Regelbetrieb kommuniziert das Webportal mit dem aus dem Internet nicht erreichbaren zentralen Verfahren zur Kraftfahrzeug-Zulassung, genauer gesagt mit der zentralen Datenbank dieses Verfahrens. Das ist erforderlich, um erfolgreiche Reservierungen zu hinterlegen bzw. freie Kennzeichen aus dem Datenbestand abzufragen. Der Angriff erfolgte – wahrscheinlich automatisch durch eine Hackersoftware – über das Webportal per sogenannter „SQL-Injection“, einer Angriffsmethode, gegen die die Software des Herstellers ekom21 offensichtlich nicht abgesichert war.

Es wurde Strafanzeige beim Landeskriminalamt erstattet, das die Ermittlungen aufgenommen und mit forensischen Untersuchungen begonnen hat. Inzwischen werden die Ermittlungen von der Generalstaatsanwaltschaft in Koblenz geleitet.

Zu Frage 2:

Es war dem Angreifer möglich, einen unzulässigen Eintrag in der Datenbank des Wunschkennzeichens vorzunehmen. Die Datenbank für das Wunschkennzeichen galt damit als kompromittiert. Um einen Schaden im oder am eigentlichen Kfz-Zulassungsverfahren auszuschließen, das – wie erwähnt – nicht über das Internet, sondern nur aus den gesicherten Netzen der Zulassungsstellen zu erreichen ist, hat der LDI als Betreiber in Abstimmung mit der KommWIS das Verfahren vom Netz getrennt, um durch Untersuchungen einen Schaden ausschließen zu können und das eigentliche Verfahren einem eventuell möglichen Angriff zu entziehen.

Druck: Landtag Rheinland-Pfalz, 25. August 2015

Für die vom LDI betrieblich verantwortete IT-Infrastruktur des Kfz-Zulassungsverfahrens kann ein unzulässiger Datenabfluss im Zuge des Angriffs nach derzeitigem Erkenntnisstand mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden. Eine abschließende Aussage bleibt allerdings dem laufenden Ermittlungsverfahren und den damit verbundenen forensischen Analysen vorbehalten.

Allgemein gilt Folgendes: Ein gewisses Gefährdungspotenzial besteht grundsätzlich immer dann, wenn – was bei den Kfz-Wunschkennzeichen gewollt ist – ein Verfahren für alle Nutzer aus dem Internet frei zugänglich ist. Eine Gefährdung ist hier systemimmanent, da Sicherheitslücken in Softwareprodukten niemals völlig auszuschließen sind. Zwar wurden die standardmäßigen Schutzmaßnahmen (z. B. Platzierung in einer sogenannten „demilitarisierten Zone“, Nutzung einer Firewall, verschlüsselte Kommunikation, etc.) auch im konkreten Fall eingesetzt. Diese Vorkehrungen können aber bei Sicherheitslücken in der eigentlichen Software keine abschließende Sicherheit gewähren. Seitens der Anwender ist eine umfassende Analyse jeder eingesetzten Software weder technisch noch rechtlich möglich.

Zu Frage 3:

Bei den Behörden der Gemeinden und Gemeindeverbände liegt die Verantwortung für den Schutz vor Hackerangriffen in der Verantwortung des jeweiligen kommunalen Trägers. Das Land unterstützt die kommunalen Gebietskörperschaften bei dieser Aufgabe u. a. durch die finanzielle Förderung des Projekts „Informationssicherheit in den Kommunalverwaltungen“ sowie durch die Zusammenarbeit mit der Zentralstelle für IT und Multimedia im Ministerium des Innern, für Sport und Infrastruktur.

Das Kernziel des Projekts „Informationssicherheit in den Kommunalverwaltungen“ ist die Erhöhung des IT-Sicherheitsniveaus in allen Gemeinden und Gemeindeverbänden. Die kommunalen Gebietskörperschaften sind und bleiben selbst verantwortlich für alle Umsetzungsmaßnahmen im Bereich der Informationssicherheit. Es sollen über das Projekt Hilfestellungen erarbeitet und Grundlagen für eine kontinuierliche und nachhaltige Verbesserung der Informationssicherheit geschaffen werden. Ebenfalls wird ein Konzept für ein kommunales CERT (Computer Emergency Response Team) entwickelt. Dabei sollen die Erfahrungen des Landes (CERT-rlp) genutzt werden. Weiterhin erfolgt eine Zusammenarbeit des Landes mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den kommunalen Spitzenverbänden. Hierbei liegt der Schwerpunkt der Kooperation im Aufbau eines für mittlere und kleinere Kommunen geeigneten IT-Grundschutzes.

Bei den Behörden des Landes wurden zur Sicherung der IT-Infrastruktur neben umfangreichen technischen auch organisatorische Maßnahmen umgesetzt. Durch eine Zertifizierung des Betriebs des rlp-Netzes nach ISO 27001 auf der Basis von IT-Grundschutz kann belegt werden, dass sämtliche vom BSI geforderten Maßnahmen zur Gewährleistung des Schutzes der Daten vor technischem Missbrauch im Landesnetz, das vom LDI administriert wird, umgesetzt wurden und permanent überprüft werden.

Auf Bundesebene wurden im IT-Planungsrat Maßnahmen zusammengetragen, die zur Sicherheit der Daten beitragen können. Diese Vorgaben wurden in Rheinland-Pfalz bereits umgesetzt. In einigen Punkten (z. B. Aufbau eine Landes-CERTs) konnte Rheinland-Pfalz bereits einige Jahre vor anderen Ländern die Vorgabe des IT-Planungsrats als erledigt melden. Die im LDI eingerichtete CERT-Kopfstelle des Landes arbeitet eng mit den Sicherheitsverantwortlichen der Ressorts zusammen und stellt im Auftrag des Ministeriums des Innern, für Sport und Infrastruktur im Intranet auch eine entsprechende Sicherheitsplattform zur Verfügung.

Zu den vom LDI elektronisch verarbeiteten Daten gehören in großem Umfang auch Daten mit Personenbezug. Es ist jeweils sichergestellt, dass die elektronische Verarbeitung dieser Daten nach Maßgabe des Landesdatenschutzgesetzes sowie gegebenenfalls weiterer einschlägiger datenschutzrechtlicher Vorschriften erfolgt. Die technische Umsetzung wird im Rahmen der BSI-Zertifizierung des Betriebs des rlp-Netzes durch externe Auditoren jährlich (Überwachungsaudit) betrachtet.

Des Weiteren hat der LDI unter Einbindung des Landeskriminalamts bauliche Maßnahmen gegen ein unerlaubtes Eindringen in die datenhaltenden Bereiche getroffen. Das Gesamtsicherheitskonzept wird abgerundet durch den Einsatz von technischen Angriffserkennungs- und Auswertesystemen, über die Angriffe registriert, analysiert und nachverfolgt werden können.

Zu Frage 4:

Als Hackerangriff im Sinne der Fragestellung ist das unberechtigte Eindringen in Computer bzw. Computernetze zu verstehen. Die Gefährdungslage in diesem Bereich ist und bleibt kritisch. Werkzeuge zur Ausnutzung von Sicherheitslücken stehen einer immer größer werdenden Anzahl an Angreifern zur Verfügung. Im Fadenkreuz der Angriffe stehen sowohl Bürgerinnen und Bürger als auch staatliche Stellen, Forschungseinrichtungen, Wirtschaftsunternehmen sowie Betreiber Kritischer Infrastrukturen (KRITIS) in Deutschland.

Mit der zunehmenden Digitalisierung und Vernetzung vieler Lebens- und Arbeitsbereiche geht eine sich dynamisch entwickelnde Gefährdungslage einher. Es ist zu beobachten, dass Wirtschaft und Verwaltung zunehmend von sehr versierten IT-Angriffen betroffen sind, die mit erheblichem Ressourceneinsatz und großer Professionalität ausgeführt werden. Solche Angriffe sind meist nur schwer zu erkennen und abzuwehren. Die offene Struktur, die technischen Möglichkeiten und die Anonymität sind Ursachen dafür, dass das Internet als Angriffsplattform missbraucht wird. Dies spiegelt sich auch in der Masse der heutigen Cyber-Angriffe wider. Für erfolgreiche Cyber-Angriffe wird nicht mehr als ein PC mit Internetanschluss benötigt. Dieser eher kleinen Investition stehen die vielfältigen Möglichkeiten gegenüber, durch kriminelle Handlungen Geld zu verdienen, vertrauliche Informationen zu erlangen oder Sabotageakte durchzuführen.

Die Professionalisierung und Separierung unterschiedlicher Aufgaben im Bereich der Cyber-Kriminalität nimmt weiter zu. Ein Cyber-Angriff kann so arbeitsteilig von verschiedenen Personen oder Gruppen, die sich auf einzelne Schwerpunkte spezialisiert haben, unabhängig voneinander realisiert werden. So gibt es beispielsweise:

- Hacker, die neue Schwachstellen in weitverbreiteten Software-Produkten suchen und diese zum Verkauf anbieten,
- Entwickler, die zu diesen Schwachstellen passende Schadsoftware oder Werkzeuge zur Generierung von Schadsoftware entwickeln und anpassen,
- Angreifer, die diese Schadsoftware einsetzen, um Informationen auszuspionieren und
- Kriminelle, die die gestohlenen Informationen kaufen, ausnutzen und zu Geld machen.

So kann selbst ein unerfahrener Angreifer ohne technisches Know-How professionelle Angriffe auf gewünschte Ziele durchführen oder durchführen lassen, ohne sich mit technischen Details und der Ausführung befassen zu müssen. Generell können drei Angreifer-Typen unterschieden werden: Kriminelle, Nachrichtendienste und sogenannte „Hacktivisten“, die durch ihre Aktionen auf angebliche gesellschaftliche, soziale, wirtschaftliche oder technische Missstände aufmerksam machen wollen. Eine Besonderheit bilden Innentäter. Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Feldern Land, See, Luft und Weltraum angesehen.

Über die bekannten Bedrohungslagen hinaus muss im Übrigen zusätzlich mit einem großen Dunkelfeld gerechnet werden.

In Vertretung:
Randolf Stich
Staatssekretär