Bayerischer Landtag

17. Wahlperiode

24.05.2017 17/16078

Schriftliche Anfrage

des Abgeordneten **Klaus Adelt SPD**
vom 23.01.2017

Hackerangriffe in Bayern

Ich frage die Staatsregierung:

1.1 Wie häufig wurden nach Kenntnisstand der bayerischen Sicherheitsbehörden in den letzten fünf Jahren bayerische Unternehmen Opfer von Hackerangriffen (bitte aufgelistet nach Regierungsbezirken)?
1.2 Welcher finanzielle Schaden entstand schätzungsweise durch diese Angriffe?

2.1 Inwieweit konnte seitens der Sicherheitsbehörden ermittelt werden, aus welchen Ländern diese Angriffe erfolgten?
2.2 Konnten – auch in Kooperation mit internationalen Strafverfolgungsbehörden – Täter ermittelt und dingfest gemacht werden?
2.3 Sofern bekannt, welche Ziele verfolgten die Hacker bei diesen Angriffen?

3.1 Wie häufig wurden nach Kenntnisstand der bayerischen Sicherheitsbehörden in den letzten fünf Jahren Einrichtungen des Freistaates Bayern Opfer von Hackerangriffen?
3.2 Um welche Einrichtungen handelte es sich dabei?
3.3 Welcher Schaden wurde durch diese Angriffe schätzungsweise verursacht?

4.1 Konnten, Bezug nehmend auf die Fragen 3.1 bis 3.3, Täter ermittelt und dingfest gemacht werden?
4.2 Inwieweit konnte ermittelt werden, aus welchen Ländern diese Angriffe erfolgten?
4.3 Sofern bekannt, welche Ziele verfolgten die Hacker bei diesen Angriffen?

Antwort

des Staatsministeriums des Innern, für Bau und Verkehr
vom 15.03.2017

Die Schriftliche Anfrage wird im Einvernehmen mit dem Staatsministerium der Justiz und dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat wie folgt beantwortet:

1.1 Wie häufig wurden nach Kenntnisstand der bayerischen Sicherheitsbehörden in den letzten fünf Jahren bayerische Unternehmen Opfer von Hackerangriffen (bitte aufgelistet nach Regierungsbezirken)?

Der Begriff „Hacking“ ist strafrechtlich nicht definiert und wird daher über verschiedenste Straftatbestände des Strafgesetzbuches abgebildet. Eine besondere Bedeutung kommt hierbei den Delikten § 202a Strafgesetzbuch (StGB) (Ausspähen von Daten), § 202c StGB (Vorbereiten des Ausspähens und Abfangen von Daten), § 303a StGB (Datenveränderung) sowie § 303b StGB (Computersabotage) zu. Zwar wird umgangssprachlich § 202c StGB als sog. „Hackerparagraf“ oder „Hackertoolparagraf“ bezeichnet, jedoch erfasst auch diese Norm nur einen Teilbereich des Phänomens „Hacking“ i. S. d. Veränderns und Zugreifens auf ein System.

Eine Recherche der relevanten Deliktsbereiche in Bezug auf bayerische Unternehmen (als Opferdaten) ist in der Polizeilichen Kriminalstatistik nicht möglich. Aus diesem Grund sind keine validen Aussagen zum Ausmaß von „Hackerangriffen“ auf bayerische Unternehmen möglich.

Grundsätzlich ist davon auszugehen, dass zahlreiche Angriffe den Sicherheitsbehörden unbekannt bleiben, weil sie von Unternehmen nicht mitgeteilt werden. Von einer Meldung wird häufig abgesehen, weil elektronische Angriffe entweder nicht erkannt werden oder Unternehmen einen Reputationsverlust und negative Auswirkungen auf den Markt bei Bekanntwerden befürchten.

Neben der Polizei steht deswegen das beim Bayerischen Landesamt für Verfassungsschutz (BayLfV) angesiedelte Cyber-Allianz-Zentrum (CAZ) Unternehmen und Betreibern kritischer Infrastrukturen auf partnerschaftlicher Basis als Ansprechpartner bei Cyberangriffen zur Verfügung. Das CAZ erfasst seit seiner Gründung (01.07.2013) die Anzahl der elektronischen Angriffe, die von Unternehmen, Hochschulen bzw. Forschungseinrichtungen und Betreibern kritischer Infrastrukturen freiwillig gemeldet werden. In die Statistik sind auch Fälle einbezogen, die von IT-Dienstleistern und Partnerdiensten mitgeteilt werden. Die Zahl der gemeldeten Angriffe und die Zahl der bearbeiteten Fälle, in denen sich der Verdacht eines nachrichtendienstlichen Hintergrunds des Angriffs ergeben hat, ist der folgenden Tabelle zu entnehmen. Eine Auflistung nach Regierungsbezirken liegt nicht vor.

Jahr	**gemeldete Angriffe**	**davon:** Verdacht eines nachrichtendienstlichen Hintergrunds festgestellt
2013/14 (01.07.2013–31.12.2014)	64	49
2015	51	41
2016	84	47

Abb. 1: an das CAZ seit Gründung gemeldete elektronische Angriffe gesamt

1.2 Welcher finanzielle Schaden entstand schätzungsweise durch diese Angriffe?

Aussagen zur finanziellen Schadenshöhe von polizeilich angezeigten Vorfällen sind aus den unter der Ziffer 1.1 genannten Gründen nicht möglich. Dem CAZ werden grundsätzlich keine Schadenssummen von den betroffenen Unternehmen genannt.

2.1 Inwieweit konnte seitens der Sicherheitsbehörden ermittelt werden, aus welchen Ländern diese Angriffe erfolgten?

In den letzten fünf Jahren wurden beim BayLfV/CAZ tatsächliche Anhaltspunkte für Angriffe aus Russland, der Volksrepublik China und dem Iran festgestellt. Darüber hinaus gab es weitere Angriffe aus verschiedenen Ländern, bei denen der Ursprung des Angriffs nicht klar zugeordnet werden konnte.

2.2 Konnten – auch in Kooperation mit internationalen Strafverfolgungsbehörden – Täter ermittelt und dingfest gemacht werden?

Ermittlungen zur Bekämpfung von Cyberkriminalität führen immer wieder zur Identifizierung von Tatverdächtigen. Auch in Zusammenarbeit mit ausländischen Sicherheitsbehörden konnten Tatverdächtige ermittelt und festgestellt werden. Internationale Behörden wie Europol liefern stetig Informationen für weitere Ermittlungsansätze und unterstützen bei der Informationsbeschaffung.

Bei Angriffen durch ausländische Nachrichtendienste ist oftmals ein Rückschluss auf konkrete Personen nicht möglich. Das BayLfV verfolgt das Ziel, den Modus Operandi der Angreifer aufzuklären. Bei klaren Indizien werden die beim BayLfV vorhandenen Informationen dem Generalbundesanwalt (GBA) mit dem Ziel der Einleitung eines Ermittlungsverfahrens weitergeleitet.

2.3 Sofern bekannt, welche Ziele verfolgten die Hacker bei diesen Angriffen?

Die Motivation der Täter kann verschiedenste Hintergründe haben. Ziele dabei können politische Motive, Machtdemonstration oder die Beibringung eines finanziellen Schadens zum Nachteil des angegriffenen Unternehmens sein.

Die Ziele von Cyberangriffen, die von Angreifern mit nachrichtendienstlichem Hintergrund gegen Unternehmen geführt werden, betreffen den Bereich von Wirtschaftsspionage. Diese elektronischen Angriffe dienen der Informationsbeschaffung.

3.1 Wie häufig wurden nach Kenntnisstand der bayerischen Sicherheitsbehörden in den letzten fünf Jahren Einrichtungen des Freistaates Bayern Opfer von Hackerangriffen?

An das bayerische Behördennetz sind alle Staatsbehörden sowie mehr als die Hälfte der bayerischen Kommunen angeschlossen. An der Schnittstelle des Behördennetzes zum Internet sind täglich mehr als 40.000 Angriffsversuche zu verzeichnen, von denen mehr als 99,99 Prozent durch aufwendige Sicherheitseinrichtungen erfolgreich abgewehrt werden. Die verbleibenden 0,01 Prozent der Angriffsversuche führten zu tatsächlichen internen Sicherheitsvorfällen, die umgehend einer erfolgreichen und effektiven Vorfallsbehandlung zugeführt wurden.

Seit Dezember 2015 sind stark zunehmende Angriffe mit sog. Verschlüsselungs-Trojanern feststellbar.

3.2 Um welche Einrichtungen handelte es sich dabei?

Staatliche Einrichtungen aller Ressorts waren direkt oder indirekt von Hackerangriffen betroffen. Im Falle der aktuell vermehrt stattfindenden Angriffe mit Verschlüsselungs-Trojanern waren z. B. die Ressorts Staatsministerium für Arbeit und Soziales, Familie und Integration, Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst, Staatsministerium für Ernährung, Landwirtschaft und Forsten, Staatsministerium der Finanzen, für Landesentwicklung und Heimat, Staatsministerium der Justiz und das Staatsministerium für Umwelt und Verbraucherschutz betroffen. Ergänzend möchten wir auf die Antwort des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat vom 03.06.2016 auf die Schriftliche Anfrage des Herrn Abgeordneten Florian Ritter vom 21.03.2016 zum Thema „Krypto-Trojaner in Bayern“ verweisen (Drs. 17/11799 vom 19.07.2016).

3.3 Welcher Schaden wurde durch diese Angriffe schätzungsweise verursacht?

Es entstand kein wirtschaftlicher Schaden.

4.1 Konnten, Bezug nehmend auf die Fragen 3.1 bis 3.3, Täter ermittelt und dingfest gemacht werden?

Nein.

4.2 Inwieweit konnte ermittelt werden, aus welchen Ländern diese Angriffe erfolgten?

Siehe hierzu Ziffer 4.1.

4.3 Sofern bekannt, welche Ziele verfolgten die Hacker bei diesen Angriffen?

In den meisten Fällen ist von wirtschaftlichen Interessen oder vorsätzlicher Störung auszugehen.