Bayerischer Landtag

17. Wahlperiode

09.05.2017 17/15870

Schriftliche Anfrage

des Abgeordneten **Florian von Brunn SPD**
vom 16.01.2017

Online-Verbraucherschutz I: Was unternimmt die Staatsregierung gegen per „Online-Skimming“ gehackte Online-Shops?

Mit Pressemitteilung vom 9. Januar 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor „aktuell mindestens 1.000 deutschen Online-Shops“ gewarnt, die vom sogenannten „Online-Skimming“ betroffen sind. Dabei nutzen kriminelle Hacker laut BSI veraltete Shop-Software, um schädlichen Programmcode einzuschleusen, und spähen damit Zahlungsinformationen der Kunden beim Bestellvorgang aus. Betroffen sind laut BSI „Online-Shops, die auf der weitverbreiteten Software Magento“ basieren.

Das CERT-Bund (Computer Emergency Response Team ...) des BSI warnte nach eigenen Angaben bereits im September 2016 die Netzbetreiber der in Deutschland betroffenen Online-Shops. Die Verantwortung liegt bei den Betreibern der Shops. Sie sind laut BSI nach § 13 Abs. 7 des Telemediengesetzes (TMG) verpflichtet, ihr System nach dem Stand der Technik gegen Angriffe zu schützen. Dazu zählt insbesondere das Einspielen von Patches zur Fehlerbehebung und Sicherheitsupdates.

Das Bundesamt zieht aber jetzt im Januar eine ernüchternde Bilanz: „Aktuellen Erkenntnissen zufolge wurde diese Infektion von vielen Betreibern bis heute nicht entfernt oder die Server wurden erneut kompromittiert.“ Damit bleiben in vielen Fällen die Gefahren für Verbraucherinnen und Verbraucher bestehen, dass ihre Zahlungsdaten und andere persönliche Informationen gestohlen und von Kriminellen missbraucht werden.

Ich frage daher die Staatsregierung:

1. a) Seit wann ist der Staatsregierung dieses o. g. Problem von per Online-Skimming gehackten Online-Shops mit der Software Magento bekannt?
   b) Welche Mitglieder der Staatsregierung wurden über diese Vorgänge persönlich informiert (bitte mit Angabe des Namens und des Ressorts)?
   c) Welche konkreten Maßnahmen hat die Staatsregierung seit dem ersten Bekanntwerden dieses Problems in Bayern ergiffen?

2. a) Sind Online-Shops betroffen, die die Sicherheitslücken noch nicht behoben haben, bei denen der Wohnsitz des Einzelunternehmers bzw. Personenunternehmers oder der Firmensitz des Unternehmens in Bayern liegen?
   b) Um welche Online-Shops handelt es sich dabei?
   c) Gehören bayerische Verbraucherinnen und Verbraucher nach Wissen der Staatsregierung zu den Geschädigten?

3. a) Wann werden Informationen zu diesem Problem in das Verbraucherinformationssystem Bayern (VIS) eingestellt, denn mit Stand 15. Januar 2016 liegen dazu noch keine entsprechenden Hinweise oder Warnungen im VIS vor?
   b) Wie werden bayerische Verbraucherinnen und Verbraucher von der Staatsregierung anderweitig vor dieser Gefahr gewarnt?
   c) Plant die Staatsregierung in diesem Zusammenhang gegenüber bayerischen Online-Shop-Betreibern Hilfestellung zu leisten oder Maßnahmen zur Abhilfe zu ergreifen, wie zum Beispiel die Einrichtung einer Beratungs-Hotline oder auch ein behördliches Einschreiten bei einer Komprimittierung des jeweiligen Shops?

4. a) Ermitteln derzeit bayerische Polizei- oder Justizbehörden gegen die Urheber solcher Manipulationen von Online-Shops?
   b) Wenn ja, welche Ermittlungserfolge gab es in diesem Kontext?
   c) Welche bayerischen Behörden sind für die Ahndung von Verstößen aufseiten der Shop-Betreiber zuständig?

5. a) Welche rechtlichen Konsequenzen kann es haben, wenn Online-Shop-Betreiber ihren o. g. rechtlichen Verpflichtungen aus dem TMG nicht nachkommen?
   b) Welche rechtlichen Möglichkeiten haben Verbraucherinnen und Verbraucher, die dadurch zu Schaden gekommen sind?
   c) An wen können sie sich zur Durchsetzung ihrer Ansprüche wenden?

6. a) Welche Maßnahmen wurden in dem o. g. Zusammenhang bereits gegen bayerischen Online-Shops ergriffen?
   b) Wie sieht das weitere Vorgehen bayerischer Behörden aus?
   c) In welcher Form findet hier die Zusammenarbeit zwischen dem BSI und bayerischen Behörden statt?

7. a) Welche politischen Schlussfolgerungen zieht die Staatsregierung aus diesen Vorfällen?
   b) Wie will die Staatsregierung Verbraucherinnen und Verbraucher besser vor solchen Gefahren schützen?
   c) Wie will die Staatsregierung in Zukunft mit Online-Shops umgehen, die ihre Verpflichtungen nach TMG nicht oder nur unzureichend erfüllen?

Antwort

des Staatsministeriums für Umwelt und Verbraucherschutz
vom 08.03.2017

Die Schriftliche Anfrage wird im Einvernehmen mit dem Staatsministerium der Justiz und dem Staatsministerium für Wirtschaft und Medien, Energie und Technologie sowie unter Beteiligung des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) wie folgt beantwortet:

1. a) Seit wann ist der Staatsregierung dieses o. g. Problem von per Online-Skimming gehackten Online-Shops mit der Software Magento bekannt?

Die Gefahren durch den Einsatz von Spähsoftware zur Erlangung von Konto- und Kreditkartendaten im Allgemeinen sind der Staatsregierung seit Längerem bekannt.

Von dem konkreten Problem im Zusammenhang mit der Software Magento und der Betroffenheit von Online-Shops hat das BayLDA aufgrund der Berichterstattung des Online-Nachrichtenmagazins heise.de am 13.10.2016 erfahren.

Die in der Anfrage beschriebenen Sicherheitslücken einer weitverbreiteten Softwarelösung für den Betrieb von Online-Shops sind sowohl im Fachreferat für Internetkriminalität im Staatsministerium der Justiz als auch der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, die regelmäßige entsprechende Fachveröffentlichungen auswertet, grundsätzlich bekannt.

b) Welche Mitglieder der Staatsregierung wurden über diese Vorgänge persönlich informiert (bitte mit Angabe des Namens und des Ressorts)?

Eine Information von Mitgliedern der Staatsregierung erfolgte nicht.

c) Welche konkreten Maßnahmen hat die Staatsregierung seit dem ersten Bekanntwerden dieses Problems in Bayern ergiffen?

Unmittelbar nach Bekanntwerden des Problems hat das BayLDA analysiert, ob bayerische verantwortliche Stellen betroffen waren. Es wurde am 24.10.2016 festgestellt, dass 15 Online-Shops in der Zuständigkeit des BayLDA betroffen waren. Alle verantwortlichen Stellen (= Shop-Betreiber) wurden daraufhin angeschrieben, über die Probleme informiert und aufgefordert, die Systeme wieder in einen nichtgehackten Zustand zu versetzen. Zusätzlich wurde Hilfe bei der Analyse angeboten, sollte ein Shop-Betreiber mit der Situation überfordert sein.

2. a) Sind Online-Shops betroffen, die die Sicherheitslücken noch nicht behoben haben, bei denen der Wohnsitz des Einzelunternehmers bzw. Personenunternehmers oder der Firmensitz des Unternehmens in Bayern liegen?

Mit Datum vom 14.02.2017 ist kein Online-Shop in Bayern, der dem BayLDA bekannt wäre, noch von der Lücke betroffen. Es kann allerdings nicht ausgeschlossen werden, dass noch weitere – dem BayLDA bislang unbekannte − Online-Shops betroffen sind.

b) Um welche Online-Shops handelt es sich dabei?

Soweit sich Frage 2 b auf Online-Shops im Sinne der Frage 2 a bezieht, entfällt eine Antwort, da derzeit keine bayerischen Online-Shops bekannt sind, die die Sicherheitslücke nicht behoben haben. Im Übrigen veröffentlicht das BayLDA nicht die Namen von Diensteanbietern und verantwortlichen Stellen, die (potentielle) Sicherheitsprobleme haben. Betroffen waren von den Sicherheitslücken nach Auskunft des BayLDA vor allem kleinere Online-Shops.

c) Gehören bayerische Verbraucherinnen und Verbraucher nach Wissen der Staatsregierung zu den Geschädigten?

Das BayLDA geht davon aus, dass auch Betroffene mit Wohnsitz in Bayern zu den Kunden der betroffenen Online-Shops gehören. Inwiefern jeder kompromittierte Shop auch zu einem Schaden für die Betroffenen führt, kann momentan noch nicht abschließend gesagt werden, da der dem BayLDA bislang bekannte Schadcode sehr generische Versuche unternimmt, personenbezogene Daten im Browser des Betroffenen abzugreifen und an einen Server im EU-Ausland zu übermitteln. Die forensische Analyse des sichergestellten Schadcodes dauert noch an.

Auch wird aufgrund der Häufigkeit des unberechtigten Zugriffs auf Kreditkartendaten und deren Missbrauchs eine eindeutige Zuordnung einer unberechtigten Abbuchung zu der Sicherheitslücke der von Online-Shops verwendeten Software Magento vermutlich nur schwer möglich sein. Hinzu kommt, dass Banken und Kreditkartenunternehmen häufig von sich aus die Verbraucher über ungewöhnliche Transaktionen informieren, wenn diese auf einen Missbrauch schließen lassen, und die erforderlichen Maßnahmen ergreifen.

3. a) Wann werden Informationen zu diesem Problem in das Verbraucherinformationssystem Bayern (VIS) eingestellt, denn mit Stand 15. Januar 2016 liegen dazu noch keine entsprechenden Hinweise oder Warnungen im VIS vor?

Im Online-Verbraucherportal www.vis.bayern.de wird der zunehmenden Digitalisierung aller Alltagsbereiche seit 2011 in der Rubrik „Internet“ mit Hintergrundinformationen und aktuellen Meldungen Rechnung getragen. Informationen zum Datensammeln und Ausspähen von Kunden- und Bezahldaten mit krimineller Zielrichtung finden sich in verschiedenen Artikeln im Verbraucherportal (z. B. „Der Missbrauch von Karten, insbes. der Maestro-Karte“; „Mit Bank- oder Kreditkarte auch als älterer Mensch zahlen? − Aber sicher!“).

Eine aktuelle Meldung zum Online-Skimming unter Verweis auf die angesprochene Pressemitteilung des BSI wurde am 18.01.2017 eingestellt. Das BSI hat seinerseits das Thema für den Endverbraucher im Newsletter vom 19.01.2017 (www.bsi-fuer-buerger.de) in der Rubrik „Prisma“ aufgenommen. Zu berücksichtigen ist allerdings, dass die Möglichkeiten der Erkennung und Vermeidung möglicher Risiken für den einzelnen Verbraucher begrenzt sind. Daher liegt ein Schwerpunkt der Informationen im VIS-Bayern darin, die Verbraucher über ihre Ansprüche und Pflichten im Falle einer missbräuchlichen Verwendung ihrer Kreditkartendaten aufzuklären und ihnen eine regelmäßige Überprüfung ihrer Zahlungskonten hinsichtlich ungewöhnlicher Zahlungsvorgänge zu empfehlen (http://www.vis.bayern.de/finanzen_versicherungen/zahlungsverkehr/index.htm).

b) Wie werden bayerische Verbraucherinnen und Verbraucher von der Staatsregierung anderweitig vor dieser Gefahr gewarnt?

Die Staatsregierung und ihre Behörden unterhalten ein breites Angebot an aktuellen Informationen zu Risiken bei der Nutzung elektronischer Dienste, das unter anderem durch die Informationsangebote der Verbraucherzentrale Bayern und des VerbraucherService Bayern ergänzt wird.

c) Plant die Staatsregierung in diesem Zusammenhang gegenüber bayerischen Online-Shop-Betreibern Hilfestellung zu leisten oder Maßnahmen zur Abhilfe zu ergreifen, wie zum Beispiel die Einrichtung einer Beratungs-Hotline oder auch ein behördliches Einschreiten bei einer Komprimittierung des jeweiligen Shops?

Es fanden bereits Hilfestellungen für die Online-Shop-Betreiber statt, die im Rahmen des o. g. aufsichtlichen Verfahrens vonseiten des BayLDA kontaktiert wurden. Zusätzlich müssen Sicherheitsmaßnahmen wie das Einspielen von aktuellen Softwareständen auf Basis § 13 Abs. 7 TMG bzw. § 9 des Bundesdatenschutzgesetzes (BDSG) zwingend durchgeführt werden. Dies wird vom BayLDA überwacht und notfalls mit aufsichtlichen Maßnahmen durchgesetzt.

Das Staatsministerium für Wirtschaft und Medien, Energie und Technologie (StMWi) hat außerdem die Industrie- und Handelskammern (IHK) und den Handelsverband über das Thema Skimming informiert und sie gebeten, die Information bei ihren Mitgliedsunternehmen weiterzuverbreiten.

4. a) Ermitteln derzeit bayerische Polizei- oder Justizbehörden gegen die Urheber solcher Manipulationen von Online-Shops?

b) Wenn ja, welche Ermittlungserfolge gab es in diesem Kontext?

Ermittlungsverfahren, welche unmittelbar das Ausnutzen der bekannten Sicherheitslücken zur Manipulation von Online-Shops zum Gegenstand haben, konnten bei der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg nicht festgestellt werden. Hierbei ist aber zu berücksichtigen, dass entsprechende Verfahren statistisch nicht gesondert erfasst werden und diese Feststellung daher nur auf der Erinnerung der Dezernenten der Zentralstelle Cybercrime Bayern beruht. Die Verwendung von nicht ausreichend aktualisierten CMS-Systemen stellt ein allgemeines Sicherheitsproblem dar, insbesondere wenn gravierende Sicherheitslücken öffentlich geworden sind (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/CMS/Studie_CMS.pdf). Die Anzeigebereitschaft von Shop-Betreibern, welche von Manipulationen betroffen waren bzw. noch sind, dürfte im Hinblick auf den drohenden Reputationsverlust überdies als gering einzuschätzen sein.

Gegenstand von Ermittlungsverfahren der Zentralstelle Cybercrime Bayern ist häufig der Einsatz von ausgespähten Kreditkartendaten. Es kann deshalb nicht ausgeschlossen werden, dass sich darunter auch solche Kreditkartendaten befinden, die über die beschriebenen Sicherheitslücken ausgespäht wurden. Ein solcher Zusammenhang lässt sich indes nicht positiv feststellen.

Ergänzend ist darauf hinzuweisen, dass mittlerweile automatisierte Lösungen existieren, welche es den Shop-Betreibern ermöglichen, auf einfache Weise zu überprüfen, ob ihre Portale von den ausgenutzten Schwachstellen betroffen sind (z. B. www.magereport.com).

c) Welche bayerischen Behörden sind für die Ahndung von Verstößen aufseiten der Shop-Betreiber zuständig?

Verstöße gegen die IT-Sicherheit bei der Verarbeitung personenbezogener Daten von verantwortlichen Stellen in Bayern fallen in die Zuständigkeit des BayLDA. Auf Grundlage des § 9 BDSG bzw. § 13 Abs. 7 TMG müssen technischen und organisatorische Maßnahmen getroffen werden, um den Schutz der personenbezogenen Daten sicherzustellen.

5. a) Welche rechtlichen Konsequenzen kann es haben, wenn Online-Shop-Betreiber ihren o. g. rechtlichen Verpflichtungen aus dem TMG nicht nachkommen?

Sollte eine verantwortliche Stelle keine geeigneten technischen und organisatorischen Maßnahmen umsetzen, so können gemäß § 38 Abs. 5 BDSG aufsichtliche Maßnahmen mit Zwangsgeldern eingesetzt werden. Auch besteht die Möglichkeit von Sanktionen bis zu 50.000 Euro bei Verstößen gegen die Anordnung technischer und organisatorischer Maßnahmen, insbesondere nach § 13 Abs.7 TMG. Eine unmittelbare Sanktionierung wegen der Nichteinhaltung der Anforderungen der Datensicherheit ist nach Auffassung des BayLDA nach derzeitiger Rechtslage nicht möglich, wird aber nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) mit einem Sanktionsrahmen von bis zu 10 Mio. Euro möglich werden.

b) Welche rechtlichen Möglichkeiten haben Verbraucherinnen und Verbraucher, die dadurch zu Schaden gekommen sind?

Wenn sich Dritte unter Ausnützen der Sicherheitslücken der von Online-Shops verwendeten Software Zugang zu Kreditkartendaten der Kunden verschaffen und damit unberechtigte Zahlungen auslösen, kann der betroffene Kunde nach § 675u Satz 2 des Bürgerlichen Gesetzbuches (BGB) von seiner Bank verlangen, den abgebuchten Betrag unverzüglich zu erstatten und die Kontobelastung zurückzuführen. Im Falle des Skimmings hat die Bank gegen den Kunden nach geltender Rechtslage auch keinen Schadensersatzanspruch gemäß § 675v BGB, sofern der Kunde nicht vorsätzlich oder grob fahrlässig seine Pflichten zum Schutz vor unbefugten Zugriffen verletzt oder gegen sonstige Bedingungen für die Nutzung der Kreditkarte verstoßen hat. Eine nicht sichere Aufbewahrung der Kreditkartendaten, die auch ohne grobe Fahrlässigkeit eine Ersatzpflicht bis zu einem Betrag von 150 Euro auslösen könnte, liegt beim Skimming nicht vor.

Daran wird sich auch durch die bevorstehende Umsetzung der Zweiten EU-Zahlungsdiensterichtlinie im Ergebnis nichts ändern, da eine Mithaftung des Kunden bei missbräuchlichen Zahlungen, sofern kein vorsätzliches oder grob fahrlässiges Verhalten vorliegt, ausgeschlossen sein wird, wenn er die missbräuchliche Verwendung der Kreditkartendaten nicht bemerken konnte. Der Kunde sollte aber in jedem Fall die missbräuchliche Verwendung seiner Kreditkartendaten seiner Bank gegenüber unverzüglich anzeigen, sobald er davon Kenntnis erlangt; hierzu ist er nach § 675l Satz 2 BGB bzw. § 675l Abs. 1 Satz 2 BGB-E (= Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz) verpflichtet.

Damit sind die Kunden vor den Folgen eines Missbrauchs ihrer Kreditkartendaten weitreichend geschützt.

c) An wen können sie sich zur Durchsetzung ihrer Ansprüche wenden?

Zur Rückerstattung unberechtigter Zahlungen gemäß § 675u BGB muss sich der Kunde an seinen Zahlungsdienstleister, d. h. seine Bank wenden.

6. a) Welche Maßnahmen wurden in dem o. g. Zusammenhang bereits gegen bayerische Online-Shops ergriffen?

Es wurden aufsichtliche Maßnahmen nach § 38 BDSG ergriffen, d. h. die verantwortlichen Stellen wurden aufgefordert, die Sicherheitsprobleme zu beseitigen und aktuelle Softwarestände einzuspielen.

b) Wie sieht das weitere Vorgehen bayerischer Behörden aus?

Das BayLDA überprüft, ob der Schadcode weiterhin (oder ggf. wieder) in den Systemen vorhanden ist. Ebenso wird überprüft, ob ein aktueller Softwarestand eingespielt wurde.

c) In welcher Form findet hier die Zusammenarbeit zwischen dem BSI und bayerischen Behörden statt?

Eine unmittelbare Zusammenarbeit zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem BayLDA gibt es bislang nicht. Dies liegt systembedingt u. a. auch daran, dass das BSI für die öffentlichen Stellen des Bundes zuständig ist und das BayLDA für die nicht-öffentlichen Stellen in Bayern. Das BayLDA nimmt die Hinweise und Empfehlungen des BSI (z. B. BSI-Grundschutz) durchaus zur Kenntnis und bezieht sie in seine Kontrollen und Bewertungen ein, soweit sie passen. Das BayLDA hat auf Anfrage beim BSI eine Liste der von den Sicherheitslücken betroffenen Online-Shops erhalten und die Informationen an die übrigen Länderbehörden weitergegeben. Das BayLDA hat das BSI außerdem gebeten, künftig über derartige Erkenntnisse unmittelbar informiert zu werden.

7. a) Welche politischen Schlussfolgerungen zieht die Staatsregierung aus diesen Vorfällen?

Aus Sicht der Staatsregierung besteht derzeit kein gesetzgeberischer Handlungsbedarf. Die Verbraucher sind durch die bestehenden und künftigen Regelungen ausreichend vor den Folgen einer missbräuchlichen Verwendung von Kreditkartendaten im Falle des Skimming geschützt. Im Zuge der Umsetzung der Verpflichtungen aus der neuen Zahlungsdiensterichtlinie der EU werden Zahlungsdienstleister künftig umfassend dazu übergehen, für Kreditkartentransaktionen im Internet eine sogenannte „starke Kundenauthentifizierung“ zu verlangen, die aufgrund der zusätzlichen Authentifizierungsmerkmale die Risiken des Ausspähens von Kreditkartendaten und missbräuchlichen Abbuchungen verringern wird. Auch sorgen die vom BSI ausgesprochenen Warnungen und Empfehlungen auf Grundlage des BSI-Gesetzes sowie die behördliche Aufsicht des Landesamts für Datenschutzaufsicht über die Anbieter auf Grundlage des Telemedien- und Bundesdatenschutzgesetzes dafür, dass Risiken durch die Verwendung unsicherer Software im E-Commerce erkannt und so weit wie möglich minimiert werden.

b) Wie will die Staatsregierung Verbraucherinnen und Verbraucher besser vor solchen Gefahren schützen?

Die Staatsregierung unterhält bereits jetzt ein umfassendes Informationsangebot für Verbraucher, das durch die Hinweise verschiedenster Stellen ergänzt wird. Die Staatsregierung wird den vorliegenden Fall zum Anlass nehmen, im Dialog mit den Interessenvereinigungen des Online-Handels das Bewusstsein für die notwendigen Maßnahmen zur Datensicherheit weiter zu stärken.

c) Wie will die Staatsregierung in Zukunft mit Online-Shops umgehen, die ihre Verpflichtungen nach TMG nicht oder nur unzureichend erfüllen?

Hierzu wird auf die Antwort zu Frage 5 a verwiesen.