**Deutscher Bundestag** **Drucksache 18/12677**

**18. Wahlperiode** 07.06.2017

# Antwort

## der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Dr. Petra Sitte, Frank Tempel, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.**
**– Drucksache 18/12392 –**

## Verbreitung von Schadsoftware über Online-Werbung („Malvertising“)

Vorbemerkung der Fragesteller

Mit der zunehmenden Bedeutung von Onlinemedien hat der Markt für Onlinewerbung immer mehr an Bedeutung gewonnen. Charakteristisch für diesen Markt, im Gegensatz zu klassischen Märkten im Print- oder Rundfunkbereich, ist die zentrale Rolle von Agenturen, die zwischen den Werbenden und den Webangeboten, auf denen Werbung geschaltet wird, vermitteln und dafür eigene Infrastruktur einsetzen. Infolgedessen ist es im Regelfall für diejenigen, die eine Webseite betreiben, nicht mehr im Einzelnen nachvollziehbar oder steuerbar, wer dort Werbung betreibt.

Dieser Umstand wird bereits seit einiger Zeit zur Verbreitung von Schadsoftware („Malware“) ausgenutzt. Diese Methode wird auch als „Malvertising“ bezeichnet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt das Problem in einer Pressemitteilung vom 29. März 2017 im Zusammenhang mit einem Angriff auf den Deutschen Bundestag wie folgt:

„Häufig wird derartige Schadsoftware verwendet, um Daten auszuspionieren oder Schaden auf dem Zielrechner zu verursachen. Eine der Hauptursachen für diese sogenannten Drive-by-Angriffe sind schädliche Werbebanner. Diese werden von unbekannten Dritten bereitgestellt oder von Agenturen vermarktet und werden häufig ohne Überprüfung oder Qualitätskontrolle in eine Webseite eingebunden. Auf diese Weise werden auch populäre und ansonsten gut abgesicherte Webseiten Ausgangspunkt von Cyber-Angriffen.“

Nach übereinstimmenden Berichten ist in den letzten Jahren eine quantitative Zunahme dieses Phänomens zu beobachten. Die Bundesregierung hat im Oktober 2016 erklärt, keine konkreten Erkenntnisse über das Ausmaß des Problems zu haben (Bundestagsdrucksache 18/10115, Antwort zu Frage 17), allerdings stellt das BSI in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2016 fest, dass Quelle von Links auf Schadprogramme „immer öfter Werbebanner“ sind (S. 18). Der weltweit durch Malvertising verursachte Schaden soll sich Schätzungen zufolge zudem auf ca. 1 Mrd. US-Dollar pro Jahr summieren (www.darkreading.com/endpoint/june-was-worst-month-of-malvertising-ever/d/d-id/1321717, Dezember 2015).

---

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 2. Juni 2017 übermittelt.*

*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

Eine zuverlässige Methode zum Schutz vor Malvertising ist die Verwendung sogenannter Ad-Blocker, also Software, die die Anzeige von über Drittserver auf Webseiten eingebundener Werbung im Browser unterbindet. Allerdings prüft die Bundesregierung gemeinsam mit den Ländern derzeit ein gesetzliches Verbot genau dieser Art von Software (vgl. Bundestagsdrucksache 18/10115). Eine abschließende Beurteilung der Bedeutung von Ad-Blockern beim Schutz vor Schadsoftware ist der Bundesregierung nach eigener Aussage nicht möglich (Bundestagsdrucksache 18/10115, Antwort zu Frage 17).

## Vorbemerkung der Bundesregierung

Die Beantwortung der Frage 3 kann aus Gründen des Staatswohls teilweise nicht in offener Form erfolgen. Aus ihrem Bekanntwerden können Rückschlüsse auf die Arbeitsweise und Methode der Nachrichtendienste des Bundes gezogen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts besonders schutzbedürftig sind (BVerfGE 124, 161 (194)). Hierdurch würde die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt, was wiederum die Sicherheit der Bundesrepublik Deutschland gefährdet. Diese Informationen werden daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Welche Erkenntnisse hat die Bundesregierung über das Ausmaß an Malvertising, den dadurch in Deutschland entstehenden Schaden und dessen zeitlicher Entwicklung?

   a) Welche Erkenntnisse hat die Bundesregierung insgesamt über den durch Schadsoftware entstehenden Schaden?

Die Fragen 1 und 1a werden gemeinsam beantwortet.

Zu dem durch Malvertising entstandenen Schaden liegen der Bundesregierung keine konkreten Informationen vor. Infektionen mit Schadsoftware werden von Nutzern häufig nicht (zeitnah) bemerkt. Zu einem späteren Zeitpunkt ist der Angriffsvektor häufig schwer nachzuvollziehen. Nur wenige Nutzer stellen Strafanzeige oder melden Vorfälle an das BSI. Die polizeilichen Statistiken weisen keine spezifischen Zahlen zu dem durch Schadsoftware entstehenden Schaden aus.

   b) Welche Erkenntnisse hat die Bundesregierung über den Anteil, den Malvertising als Auslieferemethode für Schadsoftware ausmacht, und dessen zeitlicher Entwicklung?

Die Methode, über Onlinewerbung Schadprogramme zu verbreiten, ist seit Jahren bekannt und täterseits etabliert. Sie stellt jedoch nur einen möglichen „Infektionsweg“ dar. Zu dem konkreten Ausmaß liegt der Bundesregierung keine Statistik vor.

   c) Welche Erkenntnisse hat die Bundesregierung über das Ausmaß an Malvertising im Mobilbereich und dessen Entwicklung?

Auf mobilen Endgeräten werden durch „Malvertising“ in erster Linie Warnungen vor angeblichen Schadsoftware-Infektionen eingeblendet, um die Nutzer zur Installation schädlicher Apps zu verleiten. In der Vergangenheit wurden regelmäßig

größere Malvertising-Kampagnen bekannt. Der Verlauf ist wellenförmig. Der Bundesregierung liegt kein statistisches Material zum Ausmaß und der Entwicklung des „Malvertisings“ im Mobilbereich vor.

d) Sieht die Bundesregierung die Notwendigkeit, sich mehr Informationen über das Ausmaß des Problems anzueignen, und wenn ja, welche Schritte wird sie dafür unternehmen?

Die Bundesregierung sieht die Notwendigkeit von weiteren Informationen zum Thema Malvertising. Hierzu steht das Bundesamt für Sicherheit in der Informationstechnik (BSI) in regelmäßigem Austausch mit anderen Sicherheitsteams, um Informationen über neue Malvertising-Kampagnen auszutauschen und Gegenmaßnahmen zu ergreifen. Das Bundeskriminalamt strebt generell eine Aufhellung des Dunkelfeldes im Phänomenbereich Cybercrime an und nutzt dazu z. B. auch Studien.

2. Welche Erkenntnisse hat die Bundesregierung über durch Malvertising entstehenden Schaden im Bereich der öffentlichen Verwaltung, und welche Vorfälle sind ihr dort bekannt?

Die polizeilichen Statistiken weisen keine Zahlen zum durch Schadsoftware entstehenden Schaden aus (siehe Antwort zu Frage 1a). Belastbares Material zu „Malvertising“-Vorfällen im Bereich der öffentlichen Verwaltung liegt der Bundesregierung nicht vor.

3. Welche Erkenntnisse hat die Bundesregierung darüber, dass es sich bei dem Angriff auf die IT des Deutschen Bundestages Anfang des Jahres 2017, bei dem über eine Nachrichtenseite auf eine schädliche Drittseite verlinkt wurde (siehe Pressemitteilung des BSI vom 29. März 2017), um einen Fall von Malvertising handelt?

Bei dem Angriff handelte es sich nach derzeit vorliegenden Kenntnissen der Bundesregierung nicht um Malvertising. Der entsprechende Absatz in der Pressemitteilung des BSI war ein grundsätzlicher Hinweis, der sich nicht direkt auf den vermeintlichen Angriff auf den Deutschen Bundestag bezog.

Eine weitergehende Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.*

4. Welche Empfehlungen gibt das BSI zum Schutz vor Malvertising heraus?

Das BSI veröffentlicht präventive Maßnahmen, die jede Art von webbasierten Schadcode-Angriffen verhindern sollen, darunter also auch Malvertising.

Anlassbezogen werden ggf. Informationen zu relevanten Malvertising-Kampagnen veröffentlicht. Solche Informationen werden über das Portal „BSI-für-Bürger“ zur gestellt. Empfehlung allgemeiner Schutzmaßnahmen findet sich dort z. B. auf der Seite BSI-für-Bürger. Weitere Kanäle sind technische Warnungen, der BSI-Newsletter „Sicher informiert“ und BSI Pressemitteilungen.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

5. In welcher Form und mit welchem Ergebnis ist der BSI-Expertenkreis Cyber-Sicherheit mit dem Thema Malvertising befasst?

Der BSI-Expertenkreis ist aufgrund der geringen Relevanz nicht mit dem Thema Malvertising befasst.

6. Existieren weitere Aktivitäten oder Untersuchungen seitens des BSI, die Malvertising bzw. Schutzmaßnahmen dagegen zum Gegenstand haben, und wenn ja, welche?

Malvertising ist eine Spezialform von webbasierten Angriffen. Jede Studie, Empfehlung oder Maßnahme des BSI zu webbasierten Angriffen (sogenannte Drive-By-Exploits) decken somit auch Malvertising ab.

7. Welche Empfehlungen gibt das BSI zum Einsatz von Ad-Blockern aus und hat es in der Vergangenheit herausgegeben?

In der Vergangenheit empfahl das BSI das Produkt Ad-Block Plus. Allerdings ist das Blockieren aller (somit auch legitimer) Werbebanner unverhältnismäßig und greift in das Geschäftsmodell von Content-Anbietern ein. Daher zog das BSI seine Empfehlung für Ad-Blocker zurück.

8. Welche Maßnahmen werden im Bereich der öffentlichen Verwaltung zum Schutz vor Malvertising getroffen?

In den Regierungsnetzen werden die zentralen Schutzmaßnahmen wie das Schadsoftware-Präventions-System (SPS) mit Signaturen für webbasierte Angriffe betrieben. Darüber hinaus stellt das BSI regelmäßig Informationen über Schwachstellen und Sicherheitsupdates zur Verfügung, um webbasierte Angriffe (unter die auch Malvertising fällt) zu verhindern.

9. Existieren über die Antworten zu den Fragen 4 bis 8 hinaus gegenwärtige oder geplante Maßnahmen der Bundesregierung, die den Schutz vor Malvertising zum Gegenstand haben, und wenn ja, welche?

Darüber hinaus existieren keine weiteren gegenwärtigen oder geplanten Maßnahmen der Bundesregierung.

10. Welche Anhaltspunkte hat die Bundesregierung dafür, davon auszugehen, „dass die Werbewirtschaft und die Anbieter von mit Werbung finanzierten Online-Inhalten darauf achten, dass die Nutzer durch die Übermittlung von Werbung nicht geschädigt werden“ (Bundestagsdrucksache 18/10115, Antwort zu Frage 17)?

Werden Nutzer durch die Übermittlung von Werbung geschädigt, schädigt dies nach Einschätzung der Bundesregierung den Ruf der Werbewirtschaft bzw. der Anbieter von mit Werbung finanzierten Onlineinhalten.

11. Welche konkreten gegenwärtigen oder geplanten Maßnahmen seitens der Werbewirtschaft oder von Anbietern werbefinanzierter Online-Inhalte zum Schutz vor Malvertising sind der Bundesregierung bekannt, und wie schätzt sie deren Wirksamkeit ein?

12. Sind der Bundesregierung Standards, Handlungsempfehlungen oder Selbstverpflichtungen für die Werbewirtschaft und/oder Anbieter werbefinanzierter Online-Inhalte zum Schutz vor Malvertising bekannt, und wenn ja, wie beurteilt sie diese?

Die Fragen 11 und 12 werden gemeinsam beantwortet.

Die Bundesregierung verfügt über keine konkreten Kenntnisse über die Maßnahmen der Werbewirtschaft oder von Anbietern werbefinanzierter Onlineinhalte.

13. Sieht die Bundesregierung politischen Handlungsbedarf zur Eindämmung von Malvertising, und wenn ja, in welcher Form?

Bei dem Schutz vor Schadprogrammen setzt die Bundesregierung auf Sensibilisierung und Aufklärung des Anwenders. Aufklärungsarbeit leistet das BSI. Es informiert auch über akute Gefahrenquellen.

14. Ist der Bundesregierung nach wie vor keine abschließende Beurteilung der Bedeutung von Ad-Blockern beim Schutz vor Schadsoftware möglich (Bundestagsdrucksache 18/10115, Antwort zu Frage 17)?

a) Strebt die Bundesregierung an, zu einer solchen Beurteilung zu gelangen?

Die Frage 14 und 14a werden gemeinsam beantwortet.

Die Bundesregierung sieht aus IT-Sicherheitssicht im Einsatz von Ad-Blockern eine Maßnahme zum Schutz der Nutzer im Internet, da Ad-Blocker auch vor bestimmten Angriffen durch Schadprogramme schützen können. In einer Gewichtung von Schutzmechanismen gegen die Infektion mit Schadprogrammen sind die Aktualisierung der eingesetzten Software und das Vorhandensein eines Antivirenprogrammes jedoch wichtiger. Eine abschließende Beurteilung aller rechtlichen Aspekte liegt der Bundesregierung noch nicht vor.

b) Teilt die Bundesregierung die Auffassung, dass eine solche Beurteilung zwangsläufige Voraussetzung einer gesetzlichen Regulierung von Ad-Blockern wäre?

Vor der Erwägung einer gesetzlichen Regulierung ist eine differenzierte Betrachtung möglicher Auswirkungen sinnvoll.

c) Inwieweit ist das BSI in die laufenden Prüfungen über ein Verbot von Ad-Blockern einbezogen?

Das BSI wird in Erwägungen zu einem Verbot von Ad-Blockern aufgrund seiner Expertise im Bereich IT-Sicherheit einbezogen.

15. Welche Haftungsregelungen gelten für durch Malvertising verursachte Schäden?

    a) Unter welchen Voraussetzungen müsste ein Seitenbetreiber oder eine Agentur dafür haften, dass über ihre Dienste Malvertising ausgeliefert wurde?

    b) Sind der Bundesregierung Fälle bekannt, in denen ein Haftungsanspruch erhoben oder erfolgreich durchgesetzt wurde?

    c) Welche Hindernisse sieht die Bundesregierung für die Durchsetzung derartiger Ansprüche?

    d) Sieht die Bundesregierung in dieser Frage Regelungsbedarf, und wenn ja, welchen?

Die Fragen 15 bis 15d werden zusammenhängend beantwortet.

Aufgrund der Vielzahl unterschiedlicher technischer Verfahren, mit denen Schadsoftware über Online-Werbung verbreitet wird, und den dahinter stehenden komplexen Strukturen, sind der Bundesregierung nur allgemeine Aussagen zur Haftung möglich.

Grundsätzlich gilt, dass vorrangig der Hersteller der Schadsoftware selbst nach allgemeinen deliktsrechtlichen Grundsätzen (§ 823 Absatz 1 des Bürgerlichen Gesetzbuchs – BGB, § 823 Absatz 2 BGB i. V. m. einem Schutzgesetz, § 826 BGB) für daraus resultierende Schäden an geschützten Rechtsgütern haftet. Die Haftung umfasst Schadensersatz sowie die Abwehransprüche auf Unterlassung und Beseitigung analog § 1004 BGB.

Daneben kommt eine Haftung des Betreibers derjenigen Internetseite, über die die Schadsoftware in die IT-Infrastruktur des Geschädigten gelangt ist (Seitenbetreiber), sowie des Vermittlers der Schadsoftware in Betracht:

Nach § 823 Absatz 1 BGB können Seitenbetreiber und Vermittler insbesondere dann haften, wenn sie ihnen im Einzelfall obliegende Verkehrssicherungspflichten schuldhaft verletzt haben. Denn derjenige, der in seinem Verantwortungsbereich eine Gefahrenlage schafft, die mit Gefahren für Rechtsgüter Dritter verbunden ist, hat Rücksicht auf diese Gefährdung zu nehmen und deshalb die Rechtspflicht, diejenigen Vorkehrungen zu treffen, die erforderlich und zumutbar sind, um Schädigungen zu verhindern. Verpflichtet ist grundsätzlich derjenige, der für den Bereich der Gefahrenquelle verantwortlich ist und in der Lage ist, die zur Gefahrenabwehr erforderlichen Maßnahmen zu treffen.

Welche konkreten Verkehrssicherungspflichten zu erfüllen sind, hängt von den Umständen des Einzelfalls ab. Zur Konkretisierung dieser Pflichten im Fall des Malvertising könnte § 13 Absatz 7 des Telemediengesetzes (TMG) herangezogen werden, der für Diensteanbieter Mindestanforderungen zum Schutz des Nutzers aufstellt. Ähnliche Anforderungen an die Verkehrssicherungspflicht dürften auch nach den allgemeinen Grundsätzen bestehen. Nachdem § 13 Absatz 7 TMG am 24. Juli 2015 in Kraft getreten ist, bleibt abzuwarten, ob und wie die Rechtsprechung diese Vorschrift auf Sachverhalte des Malvertising zur Anwendung bringt und hierfür konkretisiert.

§ 13 Absatz 7 TMG dürfte darüber hinaus auch als Schutzgesetz im Sinne von § 823 Absatz 2 BGB anzusehen sein, so dass bei einem Verstoß gegen die darin aufgestellten Anforderungen auch insoweit eine Haftung des Diensteanbieters in Betracht kommt.

In Einzelfällen können ggf. auch vertragliche Schadenersatzansprüche in Betracht kommen, wenn im Einzelfall, z. B. mit dem Seitenbetreiber, ein vertragliches oder vorvertragliches Rechtsverhältnis besteht und daraus erwachsende Sorgfalts- und Obhutspflichten schuldhaft verletzt werden.

Den Geschädigten treffen bei der Durchsetzung der dargestellten Haftungsansprüche die allgemeinen zivilprozessualen Risiken. Sollte er sich, abhängig von den Umständen des Einzelfalls, ggf. unzureichenden Selbstschutz entgegenhalten lassen müssen – etwa dann, wenn er es unterlassen hat, technische Schutzmaßnahmen (Antiviren-Programme, Script-Blocker, etc.) zu nutzen bzw. seine IT-Infrastruktur auf dem aktuellsten Stand (Updates von Sicherheitssoftware, Security Patches etc.) zu halten – kann er zudem Gefahr laufen wegen des Einwands der Mitverschuldens (§ 254 BGB) seinen Schaden nicht vollständig ersetzt zu erhalten.

Nach Kenntnis der Bundesregierung haben die Gerichte bisher, soweit ersichtlich, nicht über entsprechende Schadenersatzansprüche entschieden.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333