Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Sicheres Bereitstellen von Online-Werbung

Absicherung von Ad-Servern

1 Einleitung

Zur Refinanzierung von kostenfreien Inhalten auf Webseiten (z. B. von Nachrichten-Portalen) setzen Webseiten-Betreiber bevorzugt Online-Werbung ein. Ein typisches Werbemittel der Online-Werbung sind sogenannte *Werbebanner*, die beispielsweise im oberen Bereich oder im Seitenbereich einer Webseite eingeblendet werden. Für Online-Werbung existiert ein großer Markt, an dem viele Akteure beteiligt sind.

Werbetreibende (*Advertiser*) möchten ein bestimmtes Produkt bewerben und beauftragen *Agenturen*, entsprechende Werbemittel (z. B. Werbebanner) zu entwerfen. Des Weiteren beauftragen Werbetreibende *Vermarkter*, um Werbebanner auf den verschiedenen Webseiten bestmöglich zu platzieren. Dazu kaufen Vermarkter Werbeplätze bei Webseiten-Betreibern (*Publisher*) ein – und verkaufen diese wiederum an die Werbetreibenden. In der Praxis ist diese konkrete Rollenverteilung nicht immer gegeben: Beispielsweise könnte eine Agentur auch gleichzeitig als Vermarkter auftreten und das Ausliefern der Werbemittel übernehmen.

Aus technischer Sicht wird das Ausliefern von Werbemitteln von sogenannten Ad-Servern realisiert: Beim Besuch einer werbefinanzierten Webseite (z. B. ein Nachrichten-Portal) durch den Nutzer stellt die Webseite zunächst eine Verbindung zu den hinterlegten Ad-Servern her. Der Ad-Server wählt anschließend auf den Nutzer zugeschnittene Werbemittel aus und sendet diese unmittelbar an den Besucher der Webseite zurück. Die Auswahl des Werbemittels ist ein komplexer Prozess, da passende Werbemittel in Echtzeit versteigert werden (*Real-time Bidding*). Darüber hinaus werden häufig weitere, nachgelagerte Ad-Server kontaktiert, um das entsprechende Werbemittel auszuliefern oder Nutzerdaten für die Versteigerung von Werbemitteln zu erheben (*Tracking*).

2 Online-Werbung und Cyber-Sicherheit

2.1 Cyber-Angriffe über Online-Werbung

In der Vergangenheit gab es wiederholt Vorfälle, bei denen Schadprogramme in Werbebannern versteckt und verteilt worden sind (*Malvertising*). Dazu haben Angreifer beispielsweise bestehende, schlecht abgesicherte Ad-Server kompromittiert oder mittels gestohlener Kreditkarten Werbeplätze bei Vermarktern eingekauft, um schadhafte Werbemittel zu verbreiten.

Für Angreifer ist Online-Werbung ein aussichtsreicher Angriffsvektor, da durch die Verknüpfung eines Ad-Servers mit vielen Webseiten eine potenziell hohe Reichweite für die Verteilung von Schadprogrammen erzielt wird. Insbesondere besteht hier für Angreifer die Möglichkeit, Schadprogramme selbst auf seriösen Webseiten zu platzieren, sofern es gelingt, die vom Webseiten-Betreiber verlinkten Ad-Server zu kompromittieren.

Den Opfern von Malvertising droht ein großer Schaden, da es sich bei den durch Online-Werbung verbreiteten Schadprogrammen häufig um Trojanische Pferde oder Ransomware handelt. Die Trojanischen Pferde werden u. a. dazu eingesetzt, Betrug beim Online-Banking des Nutzers durchzuführen, vertrauliche Daten (z. B. Login-Informationen) auszuspähen oder massenhaft Spam-Mails zu versenden. Ransomware verschlüsselt Daten des Nutzers und fordert ihn auf, für die Entschlüsselung ein Lösegeld zu zahlen.

2.2 Hintergrund und Anwendungsbereich dieser Cyber-Sicherheitsempfehlung

Das IT-Sicherheitsgesetz dient dazu, die Sicherheit von IT-Systemen signifikant zu verbessern. Mit dem IT-Sicherheitsgesetz wurde auch eine Änderung des Telemediengesetzes (TMG) vorgenommen, um die Verantwortlichen von geschäftsmäßig angebotenen Telemedien bei der Absicherung ihrer IT-Systeme stärker in die Pflicht zu nehmen (vgl. § 13 Abs. 7 TMG).

Nach § 13 Abs. 7 TMG wie auch nach Artikel 32 der Europäischen Datenschutz-Grundverordnung (DSGVO) sind Dienstanbieter insbesondere dazu verpflichtet, konkrete Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen. Dazu gehört insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Betreiber von Ad-Servern fallen unter diese Änderung, da sie analog zu Webseiten-Betreibern auch Anbieter eines Telemediendienstes sind, die Informationen – nämlich Werbemittel – zum Abruf bereithalten. Deshalb müssen Ad-Server-Betreiber neben anderen gesetzlichen Vorgaben ebenfalls die Sicherheitsmaßnahmen nach § 13 Abs. 7 TMG und der DSGVO umsetzen.

In der Cyber-Sicherheitsempfehlung „Absicherung von Telemediendiensten nach Stand der Technik“ hat das BSI unter Beteiligung des Bitkom e. V. und des Expertenkreises Internetbetreiber der Allianz für Cyber-Sicherheit einen Katalog an Sicherheitsmaßnahmen vorgeschlagen. Dieser Katalog berücksichtigt zunächst den allgemeinen und häufigsten Anwendungsfall von Telemediendiensten – nämlich geschäftliche Webseiten – und gibt Empfehlungen, welche Maßnahmen nach dem Stand der Technik umgesetzt werden müssen.

Die vorliegende Cyber-Sicherheitsempfehlung „Sicheres Bereitstellen von Online-Werbung – Absicherung von Ad-Servern“ richtet sich nun im Speziellen an die Adressaten der Online-Werbebranche, insbesondere an Betreiber von Ad-Servern und Vermarkter. Das Dokument gibt Empfehlungen, welche technischen und organisatorischen Maßnahmen nach dem Stand der Technik zu berücksichtigen sind, um IT-Systeme der Online-Werbebranche abzusichern. Die hier vorgestellten Maßnahmen verstehen sich zum einen als Konkretisierung und zum anderen als Erweiterung der Maßnahmen, die bereits in der Cyber-Sicherheitsempfehlung „Absicherung von Telemediendiensten nach Stand der Technik“ angegeben worden sind.

3 Sicherheitsmaßnahmen

In diesem Kapitel werden die Maßnahmen zur Absicherung von Ad-Servern anhand von Beispielen kurz erläutert und enthalten zudem Referenzen zum IT-Grundschutz-Kompendium, zu Dokumenten der BSI-Standards zur Internetsicherheit (ISi-Reihe) und zu Sicherheitsempfehlungen der Allianz für Cyber-Sicherheit. Die Referenzen sollen einen Einstieg in die jeweilige Thematik einer Sicherheitsmaßnahme sowie ihrer technischen und/oder organisatorischen Umsetzung ermöglichen. Zu beachten ist hier, dass sowohl die Beispiele als auch die Referenzen einer Sicherheitsmaßnahme nicht abschließend gemeint sind.

Die folgenden Referenzen beziehen sich zunächst allgemein auf das Absichern von Ad-Servern und sind als ergänzende Hilfestellungen anzusehen:

ISi-Reihe

- ➔ Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)
- ➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- ➔ Absicherung eines Servers (ISi-Server)

Sicherheitsempfehlungen der Allianz für Cyber-Sicherheit

- ➔ #6: Basismaßnahmen der Cyber-Sicherheit
- ➔ #41: Bereitstellung von Webangeboten
- ➔ #68: Sicheres Webhosting: Handlungsempfehlungen für Webhoster
- ➔ #115: Schützen Sie sich vor professionellen gezielten Cyber-Angriffen

Open Web Application Security Project (OWASP)

- ➔ OWASP Top Ten Project
- ➔ OWASP Cheat Sheet Series

Im Folgenden werden Sicherheitsmaßnahmen aufgeführt, die aus Sicht des BSI technisch und organisatorisch umgesetzt werden MÜSSEN, um das geforderte Sicherheitsniveau nach dem Stand der Technik zu erreichen. Darüber hinaus werden Sicherheitsmaßnahmen dargestellt, die ebenfalls dem Stand der Technik entsprechen und daher aus Sicht des BSI technisch und organisatorisch umgesetzt werden SOLLTEN, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

3.1 Starke Passwörter

Für die Authentisierung am Ad-Server oder an der Werbeplattform MÜSSEN starke Passwörter (oder alternative Verfahren, die mindestens ein vergleichbares Sicherheitsniveau gewährleisten) etabliert werden. Damit soll sichergestellt werden, dass Werbekunden Passwörter einsetzen, die hinreichend stark gegenüber Brute-Force-Angriffen sind. Um solche Angriffe, bei denen alle möglichen Passwörter durchprobiert werden, zu verlangsamen, SOLLTE die Umsetzung einer sogenannten Teergrube (Tarpit) und ggf. eine Sperrung des entsprechenden Accounts berücksichtigt werden.

Um einen wirksamen Schutz gegen gestohlene Passwörter zu bieten, SOLLTE eine Mehrfaktor-Authentisierung berücksichtigt werden (z. B. bei der Authentisierung an der Verwaltungsschnittstelle des Ad-Servers).

Referenzen:

- ➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- ➔ IT-Grundschutz ORP.4: Identitäts- und Berechtigungsmanagement

3.2 Sicherheits-Updates

In der Vergangenheit ist es häufig vorgekommen, dass Ad-Server aufgrund von lange bekannten Sicherheitslücken kompromittiert wurden. Deshalb MÜSSEN Betreiber von Ad-Servern Sicherheits-Updates schnellstmöglich installieren. Diese Sicherheits-Updates MÜSSEN auf allen zum Betrieb des Ad-Servers gehörenden Komponenten sowie auf den Clients von Mitarbeitern berücksichtigt werden, um potenzielle Schwachstellen im gesamten IT-System zu beseitigen.

Der Betreiber des Ad-Servers SOLLTE einen Patchmanagement-Prozess etablieren, um bereitgestellte Sicherheits-Updates schnellstmöglich einspielen zu können.

Referenzen:

- ➔ Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- ➔ Sicherheitsempfehlung der Allianz für Cyber-Sicherheit:
  #93: Management von Schwachstellen und Sicherheitsupdates
- ➔ IT-Grundschutz OPS.1.1.3: Patch- und Änderungsmanagement

3.3 Virenschutz

Zum Schutz vor Schadprogrammen in Werbemitteln SOLLTEN Virenschutz-Programme auf den Ad-Servern eingesetzt werden. Auf Clients von Mitarbeitern MÜSSEN diese eingesetzt werden.

Auf Ad-Servern SOLLTEN Virenschutz-Programme regelmäßig nach bekannten Schadprogrammen suchen und sie ggf. isolieren bzw. entfernen. Darüber hinaus SOLLTE das Virenschutz-Programm versuchen, ein schadhaftes Werbebanner schon beim Hochladen automatisch zu erkennen und weitere Maßnahmen zu veranlassen. Dazu gehören u. a. die Überprüfung des Werbekunden und die Benachrichtigung anderer Ad-Server-Betreiber (siehe Maßnahmen „Verifizierung von Accounts“ und „Zusammenarbeit mit anderen Betreibern“).

Referenzen:

- ➔ IT-Grundschutz OPS.1.1.4: Schutz vor Schadprogrammen

3.4 Verschlüsselung

Um die Vertraulichkeit und die Integrität des Ad-Servers sicherzustellen, MUSS ein als sicher anerkanntes Verschlüsselungsverfahren eingesetzt werden. Hierbei wird zwischen der Verschlüsselung der Daten für den Transport und für die Speicherung unterschieden.

Für die Auslieferung von Werbemitteln von Ad-Servern MUSS das SSL/TLS-Protokoll eingesetzt werden, damit der Datenverkehr zwischen Web-Server und Client verschlüsselt erfolgt. Hierbei ist zu beachten, dass eine sogenannte durchgängige SSL/TLS-Unterstützung, die alle beteiligten Ad-Server in der Auslieferungskette umfasst, umgesetzt wird. Mittels automatisierter Prüfungen MUSS sichergestellt werden, dass die Auslieferungskette durch nachgelagerte Ad-Server, die keine Verschlüsselung unterstützen, nicht unterbrochen wird.

Das SSL/TLS-Protokoll MUSS auch für weitere Anwendungsfälle des Ad-Servers, insbesondere bei der Übertragung von vertraulichen Informationen, berücksichtigt werden (z. B. bei der Authentisierung an der Verwaltungsschnittstelle des Ad-Servers).

Für das Speichern von Passwörtern des Ad-Servers oder der Werbeplattform MUSS eine sichere Hashfunktion benutzt werden, damit die Daten verschlüsselt gespeichert werden. Hierzu wird auf die technischen Richtlinien „BSI TR-02102-1“ und „BSI TR-02102-2“ des BSI verwiesen.

Referenzen:

- ➔ Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls
- ➔ BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- ➔ BSI TR-02102-2 Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)
- ➔ Sicherheitsempfehlung der Allianz für Cyber-Sicherheit:
  #12: TLS/SSL Best Practice v2.0 - Allianz für Cyber-Sicherheit
- ➔ IT-Grundschutz CON.1: Kryptokonzept
- ➔ IT-Grundschutz OPS.1.2.3: Informations- und Datenträgertausch

3.5 Monitoring

In Ad-Servern MÜSSEN sicherheitsrelevante Aktivitäten unter Beachtung des Datenschutzes protokolliert werden. Beispielsweise SOLLTE überprüft werden, ob bestehende *Container Tags* (eine Menge von Skripten zur Auslieferung von Werbung und zum Erheben von Nutzerdaten) ungewöhnlich verändert oder sogar mit potenziell schadhaften Inhalten infiziert worden sind. Diese Funktion könnte automatisch, manuell oder stichprobenartig durch interne oder externe Experten der Werbebranche erfolgen. Des Weiteren könnte diese Maßnahme durch die Maßnahme „Virenschutz“ erweitert werden.

Generell MÜSSEN mit einem effektiven Monitoring Manipulationen auf den Ad-Servern nachverfolgt werden können, um bei Sicherheitsvorfällen Rückschlüsse auf Ursachen schließen zu können. Beim Monitoring (und bei allen anderen Maßnahmen) ist besonders darauf zu achten, dass bei der Verarbeitung personenbezogener Daten die Anforderungen des Datenschutzes (z. B. Löschung protokollierter Aktivitätsdaten) eingehalten werden.

Referenzen:

- ➔ Absicherung eines Servers (ISi-Server)
- ➔ IT-Grundschutz OPS.1.1.5: Protokollierung von IT-Systemen
- ➔ IT-Grundschutz DER.1: Detektion von sicherheitsrelevanten Ereignissen

3.6 Sicherheits- und Notfallvorsorge-Konzept

Der Betreiber des Ad-Servers MUSS Vorsorge treffen, um auf Sicherheitsvorfälle mit geeigneten Maßnahmen reagieren zu können. Er SOLLTE dazu über ein Sicherheits- und Notfallvorsorge-Konzept verfügen, in dem festgelegt wird, welche Strategien bzgl. der Informationssicherheit verfolgt werden. Dazu gehört insbesondere, dass der Betreiber des Ad-Servers schnellstmöglich auf Sicherheitsvorfälle reagiert, indem er schadhafte Werbemittel schnellstmöglich von seiner Werbeplattform entfernt oder den betroffenen Ad-Server schnellstmöglich abschaltet.

Falls eine Verbreitung mit schadhaften Inhalten stattgefunden hat, SOLLTEN andere Ad-Server-Betreiber (siehe Maßnahme „Zusammenarbeit mit anderen Betreibern“) informiert werden, damit diese darauf angemessen reagieren können, z. B. durch Sperren oder Löschen des schadhaften Werbemittels. Ungeachtet anderer Meldepflichten, insbesondere nach Artikel 33 der DSGVO, SOLLTE darüber hinaus das Bundesamt für Sicherheit in der Informationstechnik (BSI) über den Sicherheitsvorfall informiert werden.

Generell SOLLTE der Ad-Server-Betreiber über ein Information Security Management System (ISMS) verfügen, das Regeln definiert, um die Informationssicherheit dauerhaft zu planen, umzusetzen, zu prüfen, aufrechtzuerhalten und zu verbessern.

Referenzen:

- ➔ IT-Grundschutz DER.4: Notfallmanagement
- ➔ IT-Grundschutz DER.2.1: Behandlung von Sicherheitsvorfällen
- ➔ IT-Grundschutz ISMS.1: Sicherheitsmanagement

3.7 Sensibilisierung

Der Betreiber des Ad-Servers SOLLTE sicherstellen, dass alle Mitarbeiter ausreichende Fachkenntnisse in der Informationssicherheit haben. Für technische Mitarbeiter beinhaltet dies spezielle Kenntnisse in der Sicherheit von Online-Werbung (z. B. Klickbetrug, XSS- und SQL-Injection-Angriffe) und für alle anderen Mitarbeiter wichtige allgemeine IT-Sicherheitskenntnisse (z. B. Passwörter und Verschlüsselung, Social-Engineering-Angriffe). Der Ad-Server-Betreiber SOLLTE gewährleisten, dass sich Mitarbeiter fortlaufend über Cyber-Sicherheitsthemen informieren und fortbilden.

Referenzen:

- ➔ IT-Grundschutz ORP.3: Sensibilisierung und Schulung

3.8 Verhinderung von Tracking-Angriffen

Betreiber von Ad-Servern MÜSSEN sich an dem Grundsatz der Datensparsamkeit orientieren. Dies beinhaltet, dass nur so viele Daten erhoben werden, wie für die Auslieferung von Werbemitteln erforderlich sind.

Beispielsweise ist bekannt, dass die durch Tracking erhobenen Daten heute derart präzise sind, dass Nutzer mit einer Wahrscheinlichkeit von mehr als 99 % wiedererkannt werden können. Falls Angreifer Zugriff auf die erhobenen Nutzerdaten eines Ad-Servers erhalten sollten, könnte diese potenziell gezielte Angriffe auf bestimmte Nutzer und Nutzergruppen durchführen. Deshalb MÜSSEN die durch Tracking erhobenen Daten vor missbräuchlicher Nutzung geschützt werden.

Referenzen:

- ➔ IT-Grundschutz CON.2: Datenschutz
- ➔ IT-Grundschutz INF.1: Allgemeines Gebäude

3.9 Sperrlisten bzw. Blacklists

Der Betreiber des Ad-Servers MUSS Sperrlisten (*Blacklists*) mit URLs benutzen, hinter denen sich bekannte, schadhafte Inhalte (z. B. Ad-Server, Werbebanner) verbergen. Damit soll die automatisierte Auslieferung von manipulierten Werbekampagnen verhindert werden. Falls es einem Angreifer gelingt, manipulierte Werbemittel zu verlinken, kann diese Sperrliste direkt zum Blockieren genutzt werden.

Des Weiteren SOLLTE der Ad-Server-Betreiber eigene Sperrlisten betreiben und diese Informationen mit anderen Betreibern regelmäßig teilen, um eine möglichst hohe Anzahl an schadhaften Werbemitteln zu blockieren.

Diese Maßnahme könnte beispielsweise in die Maßnahme „Virenschutz“ integriert werden.

3.10 Verifizierung von Accounts

Der Betreiber des Ad-Servers MUSS ein Verfahren für die Verifizierung von Werbekunden etablieren. Mithilfe dieses Verfahrens soll sichergestellt werden, dass sich die Personen hinter den Werbekunden identifizieren. Diese Maßnahme soll das Erzeugen von anonymen Accounts von Werbekunden verhindern. Diese haben in der Vergangenheit häufig dazu geführt, dass mittels gestohlener Kreditkarten schadhafte Werbemittel geschaltet wurden.

Das Verifizierungsverfahren könnte durch weitere Sicherheitsmaßnahmen (z. B. „Starke Passwörter“, insbesondere Mehrfaktor-Authentisierung) erweitert werden.

3.11 Zusammenarbeit mit anderen Betreibern

Der Betreiber des Ad-Servers SOLLTE unmittelbar mit anderen Ad-Server-Betreibern und Vermarktern zusammenarbeiten. Dies beinhaltet insbesondere die Reaktion auf Sicherheitsvorfälle.

Um auf Sicherheitsvorfälle schnellstmöglich reagieren zu können, SOLLTE die Nutzung von eindeutigen, nicht personenbezogen Werbemittel-IDs diskutiert werden. Eine eindeutige Werbemittel-ID (z. B. eine ID für ein bestimmtes Werbebanner) wäre dabei über mehrere Werbenetzwerke hinweg identisch. Bei einem Sicherheitsvorfall könnte dann ein Ad-Server-Betreiber die ID des schadhaften Werbemittels anderen Ad-Server-Betreibern bekanntmachen. Diese könnten dann wiederum die Auslieferung des Werbemittels mit der entsprechenden ID in ihren Ad-Servern blockieren.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.