Westfälische Hochschule

Wissen.
Was praktisch zählt.

Erkennung webseiten-manipulierender Malware

Autoren: Tobias Urban, Norbert Pohlmann

Manipulation von Webseiten

Die Manipulation von Webseiten, insbesondere das Einschleusen von Werbung, hat in den letzten Monaten dramatisch zugenommen. Unter den 20 am häufigsten entdeckten bösartigen Objekten, welche von dem IT-Sicherheitsunternehmen Kaspersky Lab erkannt wurden, kam es zu einer explosionsartigen Erhöhung von „AdWare"-Produkten. So steigerte sich die Verbreitung von „AdWare" von lediglich 4,91 % im ersten Quartal 2014 auf 34,07 % im dritten Quartal 2015.

Gefahren durch die Webseitenmanipulation

Die größte Gefahr bei der Manipulation von Webseiten durch Malware liegt darin, dass diese auf dem Endgerät (z.B. Laptop, Smartphone oder Tablet) des Nutzers geschehen und der Nutzer nicht erkennen kann, ob wirklich alle Inhalte von einem vertrauenswürdigen Webserver bereitgestellt oder ggf. durch eine Software auf dem Nutzergerät manipuliert wurden. Abbildung 1 zeigt ein Beispiel für unberechtigt eingefügte Werbung auf der Amazon Webseite.

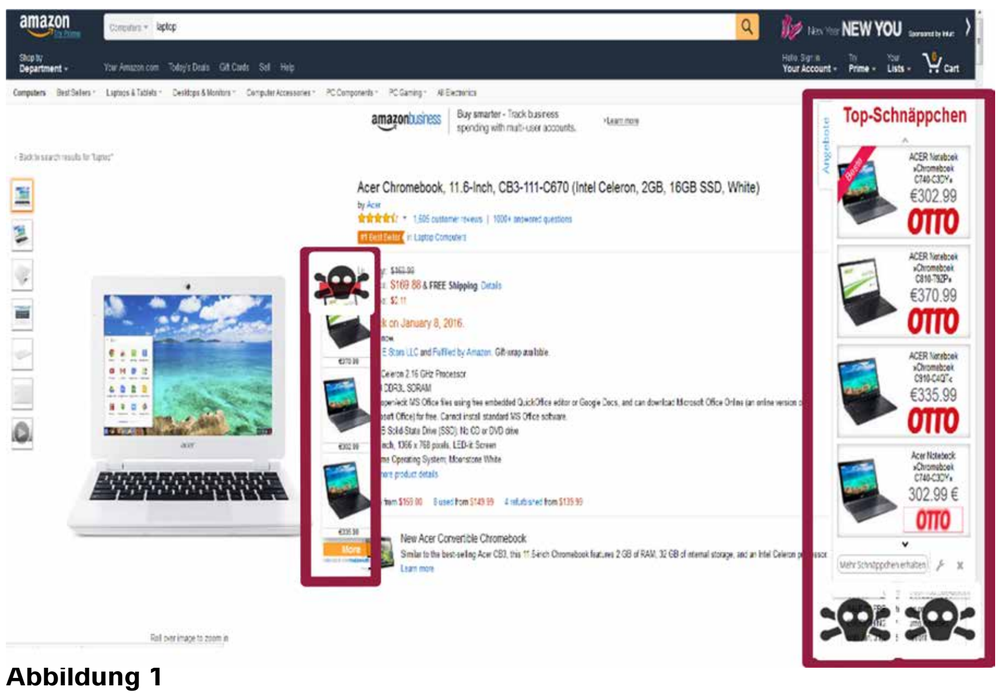

Abbildung 1
Beispiel für eine manipulierte Webseite. In die Webseite wurde clientseitig Werbebanner eingefügt (Lila Kästen). Dabei nutzt der Angreifer Werbenetzwerke die Ihn für die unberechtigte Anzeige der Werbung bezahlen. Dabei wissen die Werbenetzwerke nicht unbedingt, dass der Angreifer die Werbung unberechtigt in Webseiten einfügt.

Ziel der Forschungsarbeit

Innerhalb dieser Forschungsarbeit sollen ganzheitliche Ansätze geschaffen werden, um die Nutzer vor solchen Manipulationen zu schützen. Dabei soll das Geschäftsmodell der Entwickler und Betreiber der Malware, vor allem AdWare, analysiert, die Netzwerke, welche zum Verteilen der Werbung genutzt werden, aufgedeckt und Maßnahmen zur Erkennung und Unterbindung von Webseiten-Manipulationen geschaffen werden. Aktuelle technische Ansätze zum Schutz vor unberechtigten Veränderungen von Webseiten sind nicht ausreichend bzw. nicht praktikabel.
Die angestrebten Ziele der entwickelten Verfahren und der durchgeführten Forschungen innerhalb des Vorhabens werden nochmals in Abbildung 2 deutlich.

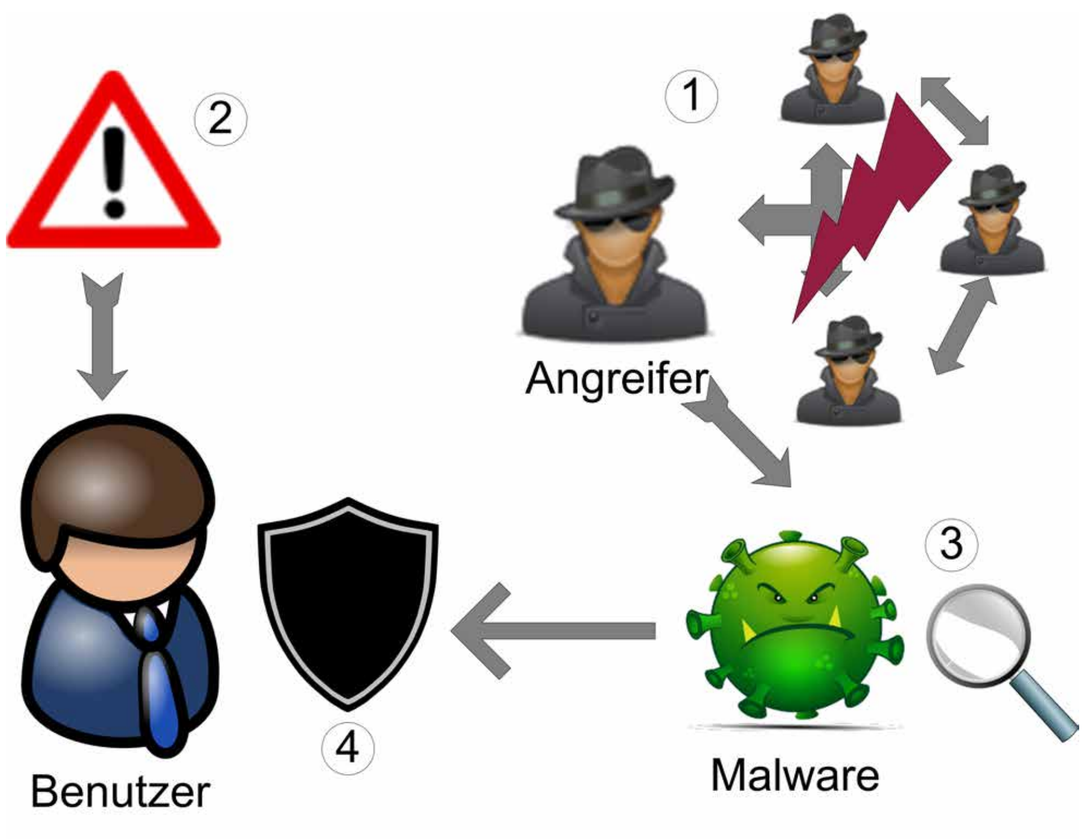

Abbildung 2
Übersicht zu den Arbeiten, die in dem Vorhaben durchgeführt werden.
- ① symbolisiert das Stören des Ökonomiemodells der Angreifer.
- Mit ② wird verdeutlicht, dass die Awareness der Benutzer gesteigert wird.
- Die Analyse der Malware wird durch ③ dargestellt.
- Der Schutz der Benutzer wird in ④ deutlich.

Kontakt

Institutsleitung
Prof. Dr. (TU NN) Norbert Pohlmann
pohlmann@internet-sicherheit.de
Tel.: +49 209 9596 - 515

Tobias Urban, M.Sc.
urban@internet-sicherheit.de
Tel.: +49 209 9596 - 857

if(is) internet-sicherheit.

Westfälische Hochschule
Fachbereich Informatik und Kommunikation
Institut für Internet-Sicherheit
www.internet-sicherheit.de