

Zusammenfassung

Dieses Dokument behandelt spezielle Bedrohungen im Internet, nämlich die Beschädigung von Webseiten. Diese Attacken sind unter dem Begriff Defiguration bekannt.

In diesem Dokument sind die wichtigsten Merkmale dieser Art von Attacke, die möglichen Auswirkungen sowie die Schutzmaßnahmen beschrieben.

Inhalt

- 1 Was ist eine Defiguration? →
- 2 Wer ist betroffen? →
- 3 Wie funktioniert eine Defiguration? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Maßnahmen →



1 Was ist eine Defiguration?

Eine Defiguration ist eine Form der Cyber-Kriminalität des Typs Cyber-Vandalismus bzw. Cyber-Terrorismus, der sich gegen eine Webseite richtet. Die Defiguration ist eine bewusste Zerstörung, Beschädigung oder Veränderung der Daten einer Webseite mit dem Ziel, maximalen Schaden und/oder Auswirkungen zu erzielen. Die Täter können politisch, religiös oder ideologisch inspiriert sein.

In der heutigen Zeit treten immer häufiger Defigurationen im Internet auf, da zahlreiche Rootkits diese Art von Attacken erleichtern, jedoch auch, weil die Zugangskosten zum Internet sinken und weil die Attacken virtuell sind (was es dem Angreifer ermöglicht, unerkant zu bleiben).

Außerdem ist eine Defiguration weitaus weniger kostspielig als die Verwendung von explosiven Materialien oder anderer Waffen.

2 Wer ist betroffen?

Jegliche Unternehmen, Organisationen oder Personen, die über einen mit dem Internet oder einem anderen Kommunikationsnetzwerk verbundenen Web-Server verfügen, können Ziel einer Defiguration sein. Es ist nicht erforderlich, über eine besonders interessante Internetseite zu verfügen. Die ganz persönliche Webseite einer Privatperson kann auch Ziel dieser Art von Attacke sein.

3 Wie funktioniert eine Defiguration?

Für die Durchführung dieser Art von Attacke stehen mehrere Mittel zur Verfügung. Der Grad ihrer Komplexität und ihr Ausmaß kann abhängig von den beabsichtigten Auswirkungen variieren.

Zu den gängigsten Mitteln zur Defiguration von Webseiten zählen die Ausnutzung von Sicherheitslücken und "semantische Attacken".

Die Mehrheit der Defigurationen erfolgt durch Ausnutzung einer auf dem Web-Server bestehenden Sicherheitslücke, die es dem Angreifer ermöglicht, den Inhalt der Webseite oder der Begrüßungsseite dieser Webseite zu verändern.

In bestimmten Fällen kann der Pirat sogar den gesamten Inhalt der Internetseite löschen.

Semantische Attacken bestehen in einer leichten Veränderung des Inhalts der verschiedenen Webseiten, um deren Sinn zu ändern. Dies hat üblicherweise zum Ziel, eine andere als die ursprüngliche Aussage zu verbreiten. Diese Änderung ist vom Verantwortlichen der Webseite (Webmaster) im Gegensatz zur einfachen Defiguration, bei der das gesamte Aussehen der Webseite verändert wird, nur schwer zu erkennen.

4 Warum sollte man sich schützen?

Da die Unternehmen in einem immer höheren Maß von den Informationsnetzwerken abhängig sind, kann die einfache Veränderung dieser Netzwerke zu nicht zu vernachlässigenden wirtschaftlichen, sozialen, logistischen, emotionalen oder auch umwelttechnischen Schäden führen. Darüber hinaus sind die

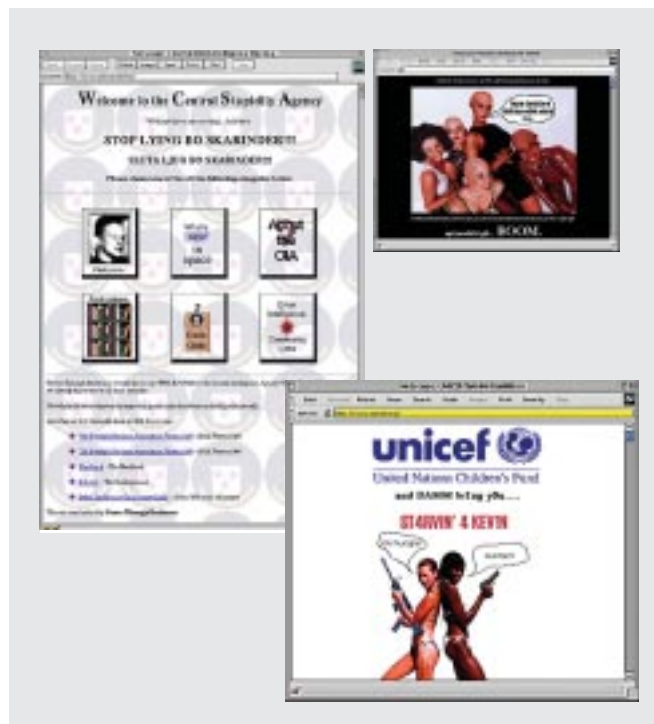
Öffentlichkeit und die Presse von jeglicher Art von EDV-Angriffen fasziniert, was zu einer umfangreichen Berichterstattung in den Medien führen kann. So führt eine Defiguration in der Tat häufig zu einem eklatanten Verfall des Markenimages des Opfers.

Beispiel:

Nach der "nicht taktischen" Bombardierung der chinesischen Botschaft in Belgrad im Jahr 1999 haben chinesische Cyber-Piraten Meldungen des Typs "Wir werden unsere Angriffe weiter fortsetzen, bis der Krieg beendet ist" auf Webseiten der amerikanischen Regierung gepostet.

Nach dem Zusammenstoß eines amerikanischen Spionageflugzeugs und eines chinesischen Abfangjägers im chinesischen Luftraum im April 2001 und der Gefangennahme der amerikanischen Besatzung in China haben sich Hacker beider Seiten einen heftigen Krieg geliefert. Mehr als 1200 amerikanische Webseiten wurden dekonfiguriert. In China war die Zahl der dekonfigurierten Internetseiten wahrscheinlich ebenso hoch.

Die Betrachtung der Konflikte zwischen Indien/Pakistan und Israel/Palästina ist ebenfalls von Interesse, wenn man bedenkt, dass die Defiguration von Webseiten die unterste Stufe von Cyber-Attentaten darstellt. Seit 1999 bis zum heutigen Tag sind immer wieder Defigurationen der Webseiten beider Parteien zu beobachten. Dabei lässt sich eine eindeutige Parallele zwischen der Anzahl der Defigurationen und den politischen und militärischen Ereignissen in den erwähnten Regionen feststellen.



5 Vorbeugende Maßnahmen

Um sich vor einer Defiguration bzw. bestimmten semantischen Attacken zu schützen, gibt es mehrere Schutzmaßnahmen:

- ➔ Verwenden Sie eine Integritätsüberwachung oder Vorrichtungen zum Schutz vor Eindringlingen. Diese Einrichtungen überprüfen, ob sich die Inhalte der Seiten einer Website einschließlich der Begrüßungsseite verändert haben.
- ➔ Installieren Sie Patches auf dem Web-Server. Sie ermöglichen eine Verringerung der Anzahl von Sicherheitslücken und somit eine Verringerung der Möglichkeit des Eindringens in den Server.

- ➔ Beauftragen Sie eine Person Ihres Vertrauens? unternehmensextern oder -intern? mit der regelmäßigen Überprüfung und Kontrolle der zu schützenden Webseite (z.B. Überprüfung der Integrität der Webseite 1 mal pro Tag).

Dank dieser Schutzmaßnahmen ist es für Sie möglich, die Wahrscheinlichkeit einer Defiguration einer Webseite zu verringern.