Malvertising-Angriffe: Wenn Hacker werben Schutzmaßnahmen gegen verseuchte Online-Anzeigen

Malvertising-Angriffe sind ein beliebtes Werkzeug für Cyberkriminelle. Häufig nutzen Hacker dabei das Vertrauen von Usern in bekannte Websites aus, um sie über legitim erscheinende Online-Werbung mit Viren, Ransomware und anderer Schadware zu infizieren. In der Vergangenheit wurde bereits eine beachtliche Liste seriöser Websites zu Trägern bösartiger Werbebanner, darunter MSN, YouTube, Spotify, Yahoo, Reuters, Forbes und die New York Times. Bei einer der jüngsten Kampagnen missbrauchten Kriminelle rund 10.000 gehackte WordPress-Seiten als Malvertising-Schleudern.

Funktionsweise von Malvertising-Angriffen

Malvertisements werden auf die gleiche Weise verbreitet wie normale Online-Werbung. Kriminelle übermitteln bösartige Grafikdateien an ein legitimes Werbenetzwerk mit der Hoffnung, dass der Werbetreibende nicht zwischen vertrauenswürdigen und schädlichen Anzeigen unterscheiden kann. Nach der Genehmigung durch den Werbetreibenden werden diese bösartigen Anzeigen an legitime Websites weitergeleitet.

In einigen Fällen registrieren Cyberkriminelle auch abgelaufene, zuvor legitime Domains neu, um sich selbst als vertrauenswürdige Domain zu tarnen. Anschließend verwenden die Kriminellen Weiterleitungen, um Nutzer auf die nun bösartige Website zu schicken. Da User beim Klick auf Anzeigen eine Weiterleitung erwarten, wirkt der Vorgang unverdächtig. Auf der bösartigen Website wird schließlich Code im Hintergrund ausgeführt, der versucht, Malware auf das Gerät des Users herunterzuladen. Diese unbeabsichtigten Downloads von Schadware werden als Drive-by-Downloads bezeichnet. Hochentwickelte Malvertising-Formen können sogar Schadware direkt von der ursprünglichen Website, welche die Online-Werbung anzeigt, auf dem Gerät des Besuchers installieren, ohne jegliche Interaktion des Opfers.

Warnzeichen für Malvertising

Cyberkriminelle werden immer raffinierter, sodass man auf den ersten Blick schwer erkennen kann, ob eine Anzeige legitim oder Teil eines Malvertising-Angriffs ist. Es gibt jedoch ein paar Warnzeichen, die auf bösartige Online-Werbung hindeuten:

- Anzeigen, die nicht so aussehen, als wurden sie von einem professionellen Grafikdesigner erstellt
- Ads, die Rechtschreibfehler aufweisen
- Werbung, die wundersame Heilmittel oder Prominentenskandale anpreisen
- Anzeigen, die nicht mit dem aktuellen oder typischen Suchverlauf oder Browserverhalten übereinstimmen

Best Practices zum Schutz vor Malvertising-Angriffen

Es gibt zudem eine Reihe von Möglichkeiten, die vor Malvertisements schützen können:

- Verwendung von Adblockern und Einschränkung von JavaScript: Wenn Anzeigen auf einer Website blockiert werden, reduziert dies natürlich das Risiko, auf eine bösartigen Werbebanner zu klicken. Allerdings sind einige Webseiten mittlerweile dazu übergangen, die Sicht auf Content zu blockieren, solange ein Adblocker aktiviert ist. Auch kann besonders fortschrittliches Malvertising Adblocker per JavaScript sowie URL-Umleitungen umgehen. Da JavaScript im Browser generell eine gewisse Gefahr birgt, kann dessen Einsatz beispielsweise mit einer Erweiterung wie „NoScript" eingeschränkt werden.

- Direkte Suche nach dem Angebot: Es empfiehlt sich generell, nicht auf Ads klicken, selbst von augenscheinlich seriösen Unternehmen. Bei Interesse an einem Angebot sollte man nach der Website des Unternehmens suchen, statt auf die Anzeige zu klicken. Wenn keine Website existiert oder Beschwerden über das Unternehmen in den Suchergebnissen auftauchen, ist die Anzeige höchstwahrscheinlich gefälscht.

- Antiviren-/Antimalwareprogramme: Obwohl diese Lösungen nicht vor allen Formen von Malware schützen können, sind sie eine gute erste Verteidigungslinie gegen bekannte Malware.

- Generell hohes Misstrauen walten lassen: Es ist wichtig, sich stets daran zu erinnern, dass reguläre Werbenetzwerke für die Verteilung sowohl von echten als auch betrügerischen Anzeigen verantwortlich sind. Die Zuverlässigkeit einer Website entscheidet nicht unbedingt darüber, ob sie bösartige Online-Werbung enthält oder nicht. Viele Beispiele zeigen, dass selbst die bekanntesten und legitimsten Websites unwissentlich Malvertisements verbreiten können. Trotz

aller Bemühungen, wird es unweigerlich Fälle geben, in denen seriöse Unternehmen Malvertisements an Benutzer verteilen.

• Verfolgen aktueller Malvertising-Skandale: Wenn sich Nutzer regelmäßig über gefährdete Websites und potenzielle Malvertising-Kampagnen informieren, bietet dies eine zusätzliche Verteidigungslinie gegen bekannte Malvertising-Bedrohungen.

Malvertising wird auch in den kommenden Jahren ein Sicherheitsproblem bleiben. Falls die Website eines Unternehmens ein Werbenetzwerk von Drittanbietern nutzt, sollten sich Verantwortliche darüber bewusst sein, dass jegliche versehentliche Verbreitung von Malvertisements auf ihrer Website potenziellen Kunden schaden und das Unternehmensimage schädigen können. Auch sollten Unternehmen ihre Mitarbeiter umfangreich über Malvertising-Angriffe im Rahmen von Sicherheitsschulungen informieren, um Infektionen auf Unternehmensrechnern sowie BYOD-Endgeräten und damit einhergehende mögliche Datenverluste zu vermeiden. Durch Aufklärung und Wachsamkeit können die Risiken von Malvertising deutlich verringert werden.