Gefährliche Webseiten: Wenn ein Klick den Computer verseucht Scheinbar harmlose - Seiten entpuppen sich als gefährliche Virenschleudern

Schon ein Klick genügt, um sich beim Besuch einer scheinbar harmlosen Internetseite zu infizieren und unbemerkt Schadsoftware auf den eigenen Rechner zu laden. Das Perfide: Viele dieser Webseiten waren kurz zuvor noch sicher und galten als ungefährlich, warnt Juraj Malcho, Chief Technology Officer bei ESET. Was Betreiber von Webseiten und Anwender tun können, um sich und andere zu schützen, hat ESET in nachfolgendem Ratgeber zusammengefasst.
Um Schadsoftware auf die Computer ihrer Opfer zu schleusen, wenden Cyberkriminelle heute immer geschicktere Methoden an. Für die Anwender wird es zunehmend schwierig, den im Internet aufgestellten Fallen zu entgehen. Denn viele der Attacken laufen über gezielt manipulierte Webseiten. "Gestern waren diese Webseiten noch sauber und heute infizieren sie den Rechner, während sie gleichzeitig die gewünschten Inhalte bereitzustellen scheinen, die man gesucht hat", umreisst ESET-CTO Juraj Malcho die Gefahr. Die Anwender bemerken davon in der Regel nichts und wissen nicht, dass die zuvor noch sichere Webseite "umgedreht" wurde und ihren Rechner längst mit gefährlicher Schadsoftware verseucht hat.

Webseitenbetreiber als unfreiwillige Helfershelfer von Kriminellen

Dabei spielt es den Kriminellen in die Hände, dass manche Webseitenbetreiber ihre Internetauftritte oft monate- oder sogar jahrelang nicht aktualisieren und dadurch versäumen, wichtige Sicherheits-Updates aufzuspielen. Deshalb werden immer öfter Sportvereine und kleine Unternehmen mit eigener Seite zum Angriffsziel der Cyberkriminellen. Sie infiltrieren oder kapern die Webseite und infizieren sie mit Schadcode. Der reine Besuch einer solchen Website kann bei nur unzureichend geschützten PCs dann bereits zu einer Infektion mit Schadcode führen.

Surfer können also nicht vorsichtig genug sein, um sich keine Schadsoftware einzufangen. Dabei bestehen gute Chancen, nicht in die Falle zu tappen. Elementar ist es, kein Betriebssystem-Update zu verpassen. Das Gleiche gilt auch für die Updates wichtiger Programme, also etwa des benutzten Office-Pakets oder des Internetbrowsers. Kein User sollte ausserdem darauf verzichten, eine Sicherheitslösung zu installieren, die manipulierte Seiten sofort beim Aufrufen erkennt. So analysiert ESET Internet Security beispielsweise den gesamten http-Traffic permanent und blockiert das Aufrufen infizierter Webseiten automatisch - und das bereits, bevor der Schadcode den Rechner erreichen kann.

So wird die eigene Webseite sicher

Wer selbst eine Website pflegt, kann mit einigen Sicherheitsmassnahmen dafür sorgen, dass die Seite nicht gekapert wird. Die meisten Attacken auf Websites werden durch die so genannte Brute Force Methode durchgeführt: Mit einer entsprechenden Software starten die Angreifer zahllose Login-Versuche, bei denen nach einem Muster von gebräuchlichen Logins und Passwörtern hin zu ungebräuchlichen Kombinationen durchgeprüft werden.
Aus diesem Grund ist es hochgefährlich, als Login für das Backend der Site leicht zu erratene Begriffe wie den eigenen Namen, Admin oder Ã„hnliches zu verwenden. Gleiches gilt für Passworte: "123456", Namen, Geburtsdaten oder Prominente erleichtern es Hackern ungemein, eine Webseite mittels Brute Force Attacke zu kapern. Der Zugang zum Webseiten-Backend sollte deshalb durch ein sicheres, starkes Passwort erschwert werden, das regelmässig ausgewechselt werden muss. Hier empfiehlt sich der Einsatz eines Passwortmanagers, der hochsichere Eingabecodes erzeugt.
Darüber hinaus schützt die Verwendung von Login Limitern Websites vor zu vielen, falschen Login-Versuchen. Wenn dann ein Krimineller mit der Brute Force Methode in die Website einbrechen will, wird er nach einer definierten Zahl nicht erfolgreicher Logins blockiert.

Wer immer von der gleichen IP auf sein Web-Backend der Website zugreift, sollte zudem sogenanntes Whitelisting nutzen: alle IPs ausser der eigenen blockieren, sodass Unbefugte nicht ins Backend gelangen können. Zusätzliche Sicherheit bietet Zwei-Faktor-Authentifizierung: Bei jedem Login ins Backend der Website wird ein Code aufs Smartphone gesendet, mit dem man den Login-Vorgang abschliessen muss.
Eine hochwertige Security-Lösung zählt ebenso zu den wichtigen Schutzmassnahmen. Für Kleinstunternehmen oder Startups empfiehlt sich hier der Einsatz des ESET Small Business Security Packs, das nicht nur PCs und Notebooks, sondern auch Smartphones, Datei- und Mailserver absichert. Nicht zuletzt gehören regelmässige Updates auch für kleine Unternehmen ins Pflichtenheft. Die Updates schliessen bestehende Sicherheitslücken und verhindern so, dass sich Cyberkriminelle über diese Schlupflöcher unbefugten Zugang verschaffen können.

Vorteile nutzen

Für Internetnutzer gilt: Wenn direkt beim Anklicken von Webseiten die Installation von Schadsoftware unterbunden wird, hat man im Vergleich zu unbedarften Opfern deutliche Vorteile. Neben der Verwendung einer entsprechend leistungsstarken Sicherheitslösung ist auch hier die Eigenverantwortung wichtig. Wer schwache Passwörter verwendet, Betriebssystem-Updates auslässt und sensible Daten nicht verschlüsselt, handelt grob fahrlässig. "Ebenso, wie man selbst auf ein regelmässiges Check-up beim Hausarzt nicht verzichten sollte, müssen auch PC, Smartphone und Co. gepflegt werden", so ESET Security-Spezialist Thomas Uhlemann. Das gilt insbesondere auch für Webseitenbetreiber, deren infizierte Internetauftritte sonst täglich tausende Webnutzer schädigen.