Router BOTNET Linux/Flasher.A

- Was ist ein BOTNET
- Wie funktioniert Linux/Flasher.A
- Bin ich betroffen?

Checkliste

- Router ermitteln
- Check des Firmewaretyps
- Aktuelle Firmware einspielen
- Absichern der Verwaltungs-oberfläche

Thomas Staffel

Bachstraße 137 • 53639 Königswinter
Tel: 0 22 23/92 26-0 • Fax: 0 22 23/92 26 26
www.indicom.de • E-Mail: info@indicom.de

WLAN-Router BOT-Net aufgedeckt

Sicherheits-Hinweis

Infizierte Router übermitteln Daten an BOTNET-Betreiber

Was ist ein BOTNET

Der Begriff BOTNET setzt sich zusammen aus den Abkürzungen von Roboter und Netzwerk. Darunter sind automatisierte Programmteile zu verstehen, die auf Rechnern oder anderer Hardware installiert sind.

Diese sogenannten BOTs sind vernetzt und leiten Daten an eine zentrale Stelle weiter bzw. erhalten von dort Befehle.

Dies geschieht in der Regel mit kriminellen Absichten und unbemerkt von den Betroffenen.

Je nachdem, welche Geräte/Computer infiziert sind, können extrem sensible Daten betroffen sein.

Aktuelle Bedrohung

In Zusammenarbeit mit dem LKA Niedersachsen hat die bekannte Computerzeitschrift c´t ein BOTNET analysiert, welches an einer sehr sensiblen Stelle im Unternehmen ansetzt, nämlich der Schnittstelle zum Internet. An dieser Stelle befindet sich üblicherweise der DSL-Router. Durch diesen wird die gesamte Unternehmenskommunikation nach außen geleitet und kann missbräuchlich verwendet werden.

Vorgehensweise

Das auf den Namen „Linux/Flasher.A" getaufte BOTNET durchsucht die ausgehende Kommunikation des Routers nach Zugangsdaten und übermittelt diese an Server des BOTNET-Betreibers. Damit können sich die Betreiber Zugriff auf die dahinter liegenden Dienste Beschaffen. Dabei sind sowohl Mailkonten aber auch Amazon- oder eBay-Accounts und Bank-Daten als Ziel denkbar.

Bin ich auch betroffen?

Die auf den DSL-Routern arbeitenden Betriebssysteme, die sogenannte Firmware, ist nicht bei allen Modellen unterschiedlich. Oft wird eine Standard-Firmware von den Herstellern nur angepasst. Betroffen sind Router, auf denen die Firmware DD-WRT installiert ist. Sie können prüfen, ob auch Ihr Router mit dieser Firmware arbeitet.

Prüfung des Routers

Unter dem Link http://www.dd-wrt.com/site/support/router-database können Sie Ihren Router prüfen. Geben Sie dazu drei Buchstaben des Routernamens in das Suchfeld ein, sie finden diesen auf dem Gerät. Sollte Ihr Router mit dieser Firmware arbeiten, wird er in der Liste aufgeführt.

Was kann ich tun?

Bei der aktuellen Bedrohung reicht es aus, den Router mit der neuesten Firmware auszustatten. Damit ist das BOTNET gelöscht. Wenn Sie konkreten Verdacht haben, ein Opfer dieses BOTNET zu sein, gibt es Möglichkeiten, die Existenz des BOTNETs nachzuweisen.

Der Angriff war nur möglich, weil viele Router Verwaltungsmöglichkeiten haben, die auch vom Internet erreichbar sind. Diese Einstellung haben sich die Betreiber des BOTNET ausgenutzt um die Router zu infizieren. Am besten schließen Sie diesen Fernwartungszugriff.

Gerne stehen wir Ihnen bei Fragen zu diesem Thema zur Verfügung. Wir beraten Sie unverbindlich zum Thema Sicherheit.

INDI COM

Thomas Staffel

Bachstraße 137 • 53639 Königswinter
Tel: 0 22 23/92 26-0 • Fax: 0 22 23/92 26 26
www.indicom.de • E-Mail: info@indicom.de