



## Ist Ihr Router in Gefahr?

*Sophos beschreibt, wie die Sicherheit des Routers zuhause gecheckt werden kann*

Paul Ducklin von Sophos hat eine Anleitung zum Check des Heimrouters verfasst. Der Hintergrund: Ein Forscher des Netzwerksicherheits-scanners Tenable fand bei einem Hack auf einen Buffalo-Heimrouter heraus, dass auch weitere 37 Router anderer Hersteller einen Firmware-Fehler enthielten. Der Fehler selbst scheint demnach bereits seit 2008 vorhanden zu sein, ohne dass er bisher bemerkt wurde. Zu den betroffenen Produkten gehören Router, die von bekannten ISPs in aller Welt ausgeliefert werden, darunter BT, Deutsche Telekom, KPN, O2, Orange, Telecom Argentina, TelMex, Telstra, Telus, Verizon und Vodafone. Für sämtliche Produkte sollten inzwischen Updates verfügbar sein, unklar ist natürlich, inwieweit diese von allen Nutzer:innen installiert wurden. Cybergangster sollen jedenfalls inzwischen auf der Suche nach anfälligen Geräten sein.

Der gesamte Naked-Security-Artikel findet sich hier:



<https://nakedsecurity.sophos.com/2021/08/10/home-and-small-business-routers-under-attack-how-to-see-if-you-are-at-risk/>

### **So kann die Sicherheit des Routers zuhause schrittweise überprüft werden:**

- Überprüfen Sie anhand der Liste von Tenable, ob Ihr Router betroffen ist. Prüfen sie auch dann, ob der Router auf dem neuesten Stand ist, wenn er nicht auf der Liste steht. Einige Internetanbieter richten ihre Router bereits so ein, dass sie sich automatisch aktualisieren. Dennoch lohnt immer ein Check, ob die Updates wie erwartet installiert und angewendet werden.
- Vermeiden Sie es, den Fernzugriff auf die Verwaltungskonsole Ihres Routers zu aktivieren. Die meisten modernen Router beschränken den Zugriff auf die Web-Konsole standardmäßig auf das interne Netzwerk, enthalten aber eine Option, mit der Sie den Fernzugriff selbst aktivieren können. Stellen Sie sicher, dass diese Option deaktiviert ist, es sei denn, Sie sind sich absolut sicher, dass Sie sie benötigen. Es macht keinen Sinn, den Webserver Ihres Routers unnötigerweise direkt dem Internet auszusetzen.
- Aktivieren Sie niemals den Fernzugriff auf Ihren Router auf Anweisung einer Ihnen unbekannt Person. Betrüger kontaktieren Sie oft per E-Mail oder Telefon und behaupten, sie seien "da, um zu helfen", und verlangen dann Fernzugriff auf Ihren Router oder Ihren Computer, um ein imaginäres "Problem" zu "beheben". Diese Betrüger behaupten oft dreist, sie kämen von Microsoft, Google, Ihrem Internetanbieter oder sogar von der Polizei. Sie können bedrohlich und aggressiv werden, wenn sie zur Rede gestellt werden. Lassen Sie sich nicht einschüchtern. Sie haben nicht um Hilfe gebeten, also müssen Sie sie auch nicht annehmen - legen Sie einfach auf oder ignorieren Sie die E-Mails und wenden Sie sich stattdessen an jemanden, den Sie kennen und dem Sie vertrauen.
- Wenn Sie ein Programmierer sind, überprüfen Sie alle Ihre Eingaben. Jede Software, die über das Netz gelieferte Daten akzeptiert, muss davon ausgehen, dass alle Eingaben, die sie erhält, mit Fallen versehen sein könnten, um nach Schwachstellen zu suchen. Bei Systembefehlen, Verzeichnissen und Dateinamen ist besondere Vorsicht geboten, da es viele Zeichen und Zeichenfolgen gibt, die eine besondere Bedeutung haben, wenn sie in diesen Zusammenhängen verwendet werden, wie z. B. die oben erwähnte berüchtigte "Punkt-Punkt"-Folge.

### **Neu: Social Media von Sophos für die Presse**

Wir haben speziell für Sie als Journalist\*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos\_info

### **Pressekontakt:**

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

[sophos@tc-communications.de](mailto:sophos@tc-communications.de)