TFTP

Möglicherweise haben Sie vor Kurzem einen Brief und/oder eine E-Mail von Sunrise erhalten, in dem/der Sie darauf hingewiesen wurden, dass ein Gerät in Ihrem Netzwerk eine Sicherheitslücke aufweist, die als «offenes TFTP» bekannt ist. Wenn Sie eine entsprechende Mitteilung von uns erhalten haben, gehen Sie bitte nach den auf dieser Seite aufgeführten Hinweisen vor, um das Problem zu beheben.

Übersicht

TFTP ist ein Dienst, der es anderen Geräten in einem Netzwerk ermöglicht, aus der Ferne auf Dateien und Ordner auf einem Gerät zuzugreifen, auf dem der Dienst läuft, ohne Anmeldedaten eingeben zu müssen. Dieser Dienst ist nur für die Nutzung in einem kleinen lokalen Netz, z. B. bei Ihnen zu Hause, vorgesehen, kann aber, wenn er mit dem Internet verbunden ist, von Dritten missbräuchlich verwendet werden.

Was ist passiert?

Wir arbeiten mit einer Reihe von gemeinnützigen Organisationen aus verschiedenen Sicherheitsbereichen zusammen, die Informationen über Geräte im Internet sammeln, die offenbar gefährdet oder falsch konfiguriert sind. Das bedeutet, dass Ihr gefährdetes oder falsch konfiguriertes Gerät im Internet öffentlich zugänglich ist und die von diesen Organisationen durchgeführten Scans daher nicht innerhalb Ihres privaten Netzwerks stattfinden.

Wir vermuten, dass ein Gerät, das an Ihr Heimnetzwerk angeschlossen ist, eine Schwachstelle in Form eines offenen TFTP aufweist. Weitere Informationen zu diesen Berichten finden Sie unter tftpscan.shadowserver.org

Wenn die entsprechenden Einstellungen offen gelassen werden, können sie zur Entwendung persönlicher Daten und zur unwissentlichen Beteiligung an bösartigen Aktivitäten ausgenutzt werden, zum Beispiel für einen DDoS-Angriff (Distributed Denial of Service).

Es ist daher wichtig, dass Sie die Ratschläge in diesem Artikel befolgen.

Hinweis: Dieser Artikel soll Ihnen als Ratgeber dienen. Sunrise ist nicht verantwortlich für allfällige Probleme, die bei der Lösung des Problems auftreten, und kann keinen technischen Support für solche Probleme leisten.

Wie kann das Problem behoben werden?

Eine Schwachstelle in Form eines offenen TFTP kann behoben werden, indem Sie in der Konfiguration Ihrer Firewall den UDP-Port 69 sperren.

Es ist zu beachten, dass die Sperrung dieses Ports nur den Datenverkehr unterbindet, der über diesen Port Ihr Heimnetzwerk verlässt oder dorthin eintritt. Die Dienste in Ihrem Zuhause, die diesen Port nutzen, sollten weiterhin wie gewohnt funktionieren.

So schliessen Sie den gefährdeten Port:

- Rufen Sie die Konfigurationsseite Ihres Routers auf.
- Melden Sie sich mit Ihrem Benutzernamen und Passwort an, die Standardeinstellungen werden auf dem Router selbst angezeigt.
- Wählen Sie die Option «Port-Weiterleitung».
- Entfernen Sie alle Regeln, durch die Port 69 offen gehalten wird.
- Wählen Sie die Option «Port-Auslösung» aus.
- Entfernen Sie alle Regeln, durch die Port 69 offen gehalten wird.

Sorgen Sie dafür, dass alle Geräte in Ihrem Netzwerk durch eine Firewall geschützt sind. Es ist wichtig, dass Sie überprüfen, ob alle Ihre Geräte hinter einer Firewall angeschlossen sind.

Version: 12.2021

Wissenswertes rund um das Thema Internetsicherheit

Sunrise ist Mitbegründerin und Mitglied von iBarry.ch: einer gemeinnützigen Organisation, die mit Experten für Online-Sicherheit zusammenarbeitet, um Ihnen alle Informationen zur Verfügung zu stellen, die Sie brauchen, damit Sie und Ihre Kinder sicher im Internet unterwegs sein können.

Weitere Informationen zu iBarry finden Sie unter https://www.ibarry.ch/de/

Version: 12.2021