SNMP

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 SNMP» (Simple Network Management Protocol) 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

SNMP (Simple Network Management Protocol) ist eine Methode, mittels derer ein Gerät in einem Computernetzwerk aus der Ferne verwaltet oder auf dieses zugegriffen werden kann. Bei einer SNMP-Schwachstelle handelt es sich um eine Sicherheitslücke, bei der ein Dritter dieses Protokoll nutzen kann, um sich zu böswilligen Zwecken unbefugten Zugang zu Ihrem Netzwerk / Ihren Geräten zu verschaffen, wenn das Protokoll falsch konfiguriert ist.

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 SNMP-Schwachstelle aufweist.

Weitere Informationen zu diesen Berichten finden Sie unter snmpscan.shadowserver.org

Wenn die entsprechenden Einstellungen offen gelassen werden, können sie 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?

Die einfachste Möglichkeit, SNMP-Bedrohungen/-Schwachstellen zu beseitigen, besteht darin, die Ports 161 und 162 der UDP-Schnittstelle in der Firewall-Konfiguration zu sperren.

Es ist zu beachten, dass die Sperrung dieser Ports nur den Datenverkehr unterbindet, der über die jeweiligen Ports Ihr Heimnetzwerk verlässt oder dorthin eintritt. Die Dienste in Ihrem Zuhause, welche die Ports 161 und 162 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 welche die Ports 161 und 162 offen gehalten werden.
- Wählen Sie die Option «Port-Auslösung» aus.
- Entfernen Sie alle Regeln, durch welche die Ports 161 und 162 offen gehalten werden.

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.

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