HeLi NET warnt: Telefonmissbrauch über Fritz!Box

Die Fritz!Box ist ein beliebter Router und Zugang ins Internet. Der regionale Telefonanbieter HeLi Net warnt aktuell vor Missbrauchsfällen, wenn dieses Gerät auch als Telefonanlage genutzt wir. Durch Manipulationen von Hackern werden unter anderem teure Auslandsgespräche abgesetzt oder kostenplichtige Dienste eingerichtet.

HeLi Net rät ihren Kunden: „Der Angriff ist nur dann möglich, wenn der Angreifer über die genaue Kombination aus Mailadresse oder FRITZ!Box-Benutzername, IP-Adresse der FRITZ!Box und Kennwörtern für Fernzugang und FRITZ!Box-Oberfläche verfügt. Möglicherweise besteht ein Zusammenhang zu dem kürzlich vom BSI veröffentlichten Diebstahl von 16 Millionen digitalen Identitäten. Betroffen sind bisher ausschließlich Anschlüsse, welche über eine für lange Zeit gleichbleibende öffentliche IPv4-Adresse eingewählt sind. Dies ist häufig bei Glasfaseranschlüssen der Fall. Bei „normalen“ DSL Anschlüssen erfolgt in der Regel eine Zwangstrennung nach 24 Stunden, wobei der Anwender eine neue IP erhält.

Probleme durch die Fernzugriffsfunktion

Ein Zugriff von außen ist nach derzeitiger Kenntnislage nur dann möglich, wenn der HTTPS-Fernzugriff (Port 443) oder der MyFRITZ!-Dienst durch den Anwender selbst eingerichtet wurde. Der Angreifer muss den Benutzernamen und das zugehörige Fernzugriffskennwort kennen. Beides hat der Anwender selbst bei der Einrichtung des Fernzugriffs vergeben und ist ausschließlich in der FRITZ!Box bekannt. Ohne Kenntnis dieses

Kennwortes ist kein Zugriff für den Angreifer möglich. Sind HTTPS-Fernzugriff (Port 443) oder MyFRITZ!-Dienst aktiviert, wird folgendes empfohlen:

• die Passwörter zu ändern.
• die Kennwörter sollten unbedingt unterschiedlich sein.
• Rechner sollten auf Schadsoftware (z.B. Trojaner) überprüft werden.
• Sollte die Telefonkonfiguration ungewöhnliche Rufumleitungen aufweisen, sollten diese sofort entfernt werden.
• Weiter wird empfohlen, eine Telefonsperre für Auslandsrufnummern einzurichten.“

Weitere Infos gibt es auch hier.