Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sicherer Einsatz von Breitband-Routern

Im Allgemeinen werden Internetzugänge mithilfe von DSL-, Kabel- oder Glasfaser-Anschlüssen realisiert. Eine Netzanbindung an diese Anschlüsse erfolgt bei kleinen und mittleren Unternehmen überwiegend durch Breitband-Router. Häufig bildet ein solcher Router die einzige zentrale und wesentliche Sicherheitskomponente zum Schutz des internen Netzes. Gelingt einem Angreifer der Zugriff auf den Router, kann er auf verschiedene Weisen Schaden verursachen, z. B. können Passwörter, E-Mails oder sonstige private Daten aus dem internen Netz ausgespäht werden. Für den Inhaber des Internetzuganges kann zudem ein erheblicher finanzieller Schaden entstehen, wenn die (VoIP-)Telefonleitung missbraucht wird, z. B. indem der Angreifer kostenpflichtige Nummern anwählt. Des Weiteren kann der eigene Internetzugang für Angriffe auf andere Internetnutzer missbraucht werden, um u. a. Spam zu versenden oder um Distributed Denial-of-Service-Angriffe (DDoS-Angriffe) auszuführen. Eine sichere Konfiguration von Routern ist daher unerlässlich.

Diese BSI-Veröffentlichung fasst wesentliche Aspekte zusammen, die beim Kauf bzw. bei der Miete eines Breitband-Routers beachtet werden sollten. Des Weiteren werden Empfehlungen für einen sicheren Betrieb von Routern ausgesprochen.

In dieser Cyber-Sicherheitsempfehlung werden die Verben „SOLLTE“ und „MUSS“ in ihren jeweiligen Formen sowie den zugehörigen Verneinungen genutzt, um deutlich zu machen, wie die jeweiligen Anforderungen zu interpretieren sind. Im Folgenden werden Sicherheitsmaßnahmen aufgeführt, die aus Sicht des BSI erfüllt werden MÜSSEN, um ein angemessenes Sicherheitsniveau nach dem Stand der Technik zu erreichen. Darüber hinaus werden Sicherheitsmaßnahmen dargestellt, die ebenfalls dem Stand der Technik entsprechen und aus Sicht des BSI grundsätzlich erfüllt werden SOLLTEN. Es kann aber Gründe geben, von einer gängigen Empfehlung abzuweichen, z. B. weil das Sicherheitsniveau durch andere Maßnahmen gewährleistet werden kann. Dies sollte aber sorgfältig abgewogen, stichhaltig begründet und dokumentiert werden.

1 Zugriffsschutz

1.1 Benutzeroberfläche

Die Benutzeroberfläche bzw. die Weboberfläche des Routers ist besonders schützenswert, da sie eine potenzielle und zugleich häufige Angriffsfläche darstellt. Bereits in der Werkseinstellung muss die Benutzeroberfläche daher mit einem individuellen, zufälligen Passwort geschützt sein, das aus mindestens 8 Zeichen besteht. Sofern die Benutzeroberfläche keinen Passwortschutz besitzt oder lediglich mit einem Standardpasswort, wie beispielsweise „admin“ oder „1234“ geschützt ist, muss bei der ersten Konfiguration

des Routers ein sicheres Passwort[1] gesetzt werden. Hierzu bieten diverse Router-Modelle einen Passwortassistenten an, der die Passwortstärke eines Passwortes anzeigt, bevor dieses übernommen wird.

Der Zugriff auf die Benutzeroberfläche sollte aus dem internen Netz über HTTPS erfolgen, sofern der Router diese Möglichkeit bietet. Nach einer erfolgreichen Anmeldung an der Benutzeroberfläche sollte auch eine Abmeldung durchgeführt werden, sobald die Benutzeroberfläche nicht mehr benötigt wird.

Ferner können viele Router auch aus dem Internet konfiguriert werden. Falls diese Möglichkeit tatsächlich erforderlich sein sollte, muss der Zugriff auf die Benutzeroberfläche über HTTPS erfolgen und somit verschlüsselt sein. Da die Benutzeroberfläche in diesem Fall einem weitaus größeren Risiko ausgesetzt ist als unter normalen Umständen, ist darauf zu achten, dass das Passwort eine höhere Passwortstärke (Länge und Komplexität) besitzt.

Um den Router vor automatisierten Angriffen, wie beispielsweise Brute-Force-Angriffe zu schützen, müssen die Anmeldeversuche an der Benutzeroberfläche des Routers zeitlich verzögert werden, nachdem eine Anmeldung fehlgeschlagen ist. Alternativ kann die Benutzeroberfläche einen CAPTCHA[2] (Completely Automated Public Turing test to tell Computers and Humans Apart) verwenden.

1.2 WLAN

Beim Einsatz von WLAN besteht ein wesentliches Problem darin, dass die Kommunikation zwischen dem Router und einem Client auch noch aus großer Distanz mitgehört werden kann. Um diese Kommunikation zu schützen, sollte der Router standardmäßig einen individuellen, zufälligen WPA2-Schlüssel (Pre-shared Key, PSK) verwenden, der aus mindestens 20 Zeichen[3] besteht. Bei Bedarf kann auch WPA2-Enterprise verwendet werden, um das WLAN abzusichern. Hierbei kommt zur Authentifizierung ein RADIUS-Server (Remote Authentication Dial-In User Service) zum Einsatz.

Moderne Router stellen einen WLAN-Gastzugang bereit, um Gästen einen eigenen Internetzugang zu ermöglichen. Diese Funktion sollte verwendet werden, um zum einen das normale WLAN vom WLAN-Gastnetz logisch zu trennen. Zum anderen kann dadurch der WPA2-Schlüssel des Gastzuganges häufiger und gleichzeitig unabhängig vom WPA2-Schlüssel des normalen WLAN geändert werden. Ein Gastzugang sollte deaktiviert werden, falls er nicht mehr benötigt wird.

2 Aktualisierung der Firmware

Außer der Bereitstellung von neuen Funktionen kann die Aktualisierung der Firmware dazu dienen, bekannte Schwachstellen des Routers zu schließen. Sowohl Router-Hersteller als auch Internet-Service-Provider (ISP) können Firmware-Updates für ihre verkauften bzw. vermieteten Router bereitstellen. Sofern der Router eine Funktion zur Verfügung stellt, um automatisch sicherheitsrelevante Firmware-Updates zu installieren, sollte diese Funktion auf der Benutzeroberfläche aktiviert werden.

Router-Besitzer, die selbständig ein Firmware-Update durchführen möchten und diese Möglichkeit auch haben, sollten regelmäßig überprüfen, ob die Firmware noch aktuell ist. Sicherheitsrelevante Firmware-Updates sollten vom Besitzer installiert werden. Ein abonnierter Newsletter des Router-Herstellers kann unter Umständen helfen, frühzeitig über ein Firmware-Update informiert zu werden.

Beim Kauf eines Routers sollten Hersteller bzw. Internet-Service-Provider präferiert werden, die in der Vergangenheit über einen Zeitraum von mindestens. 5 Jahren Software-Updates für

1 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
2 Bei einem CAPTCHA muss der Benutzer des Routers eine Aufgabe lösen, z. B. das Antippen von Bildern mit einem bestimmten Inhalt, bevor das Passwort für die Weboberfläche eingegeben werden kann.
3 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-WLAN/wlan_node.html

ihre Modelle bereitgestellt haben. Des Weiteren sollten Router-Modelle bevorzugt werden, die eine automatische Installation von sicherheitsrelevanten Firmware-Updates unterstützen.

3 Dienste und Portweiterleitungen

Moderne Router ermöglichen außer dem Zugang zum Internet eine Vielzahl zusätzlicher Funktionen. So unterstützen diverse Router Smart Home oder stellen einen Medienserver bereit. Diese Funktionen können allerdings auch ein Einfallstor für Angreifer darstellen. Daher sollten alle Dienste auf dem Router deaktiviert werden, die nicht benötigt werden. Hierzu gehören grundsätzlich die WPS-PIN-Methode (Wi-Fi Protected Setup PIN Methode) sowie UPnP-IGD[4] (Universal Plug and Play – Internet Gateway Device).

Unter Umständen können bestimmte Dienste erforderlich sein, z. B. wenn die NAS-Funktionalität (Network Attached Storage) des Routers genutzt werden soll. Hierbei wird ein Speichermedium (z. B. USB-Stick) am Router angeschlossenen und der Zugriff auf die Daten gestattet. Dabei kann der Zugriff sowohl aus dem internen Netz als auch über das Internet ermöglicht werden. Wenn der Zugriff auf notwendige Dienste mit einem Passwort abgesichert werden kann, dann sollte dies erfolgen, wobei das Passwort auch hier aus mindestens 8 Zeichen bestehen sollte. Generell müssen alle Dienste des Routers, die direkt aus dem Internet genutzt werden können, sicher konfiguriert werden, indem u. a. ein langes und zugleich komplexes Passwort vergeben wird.

Eingerichtete Portweiterleitungen im Router sollten regelmäßig auf ihre Notwendigkeit überprüft werden, um sie ggf. zu deaktivieren.

4 Telefonie

Verschiedene Router-Modelle können mittels der Benutzeroberfläche eine Sperrliste für Rufnummern (ankommende und ausgehende Anrufe) definieren. Diese Funktionalität bieten auch einige Internet-Service-Provider (ISP) über ihre Kundenportale an. Sofern keine oder selten Auslandsgespräche getätigt werden, sollten ausgehende Auslandsanrufe unter Zuhilfenahme des Routers oder des ISP-Kundenportals verhindert werden. Hierbei sollte die Sperrung über das ISP-Kundenportal präferiert werden, da sie auch bei der Kompromittierung des Routers wirkt. Ferner sollten die Rufnummernbereiche 0900 (Premium-Dienste), 0137 (Massenverkehrs-Dienste), 0180 (Service-Dienste), etc. ebenfalls mithilfe des Routers oder des ISP-Kundenportals blockiert werden, wenn diese nicht benötigt werden.

Bei Voice over IP (VoIP) werden Sprachdaten über das Internet-Protokoll (IP) übertragen, um beispielsweise das Telefonieren über das Internet zu ermöglichen. In der Regel bieten Internet-Service-Provider neben einem Internetzugang auch IP-Telefonie (VoIP) an. Des Weiteren gibt es Internet-Telefonie-Provider, die in erster Linie IP-Telefonie zur Verfügung stellen. Beide Provider stellen Ihren Kunden VoIP-Zugangsdaten inklusive Passwort bereit, die üblicherweise in einem Router eingetragen werden. Somit stellt der Router auch eine Telefonanlage zur Verfügung. Das VoIP-Passwort sollte ebenfalls aus mindestens 8 Zeichen bestehen.

Zahlreiche Router-Modelle bieten eine DECT-Basisstation an, sodass DECT-Telefone am Router registriert werden können. Bei der Konfiguration von DECT sollte eine PIN für die Anmeldung der DECT-Telefone am Router vergeben werden. Des Weiteren sollte der Router standardmäßig eine DECT-Verschlüsselung verwenden.

Mittels Callthrough können kostengünstige Gespräche mithilfe des Routers geführt werden. Hierfür wird eine Rufnummer (Callthrough-Rufnummer) im Router hinterlegt, die beispielsweise aus dem Mobilfunknetz angerufen werden kann. Sobald der Router einen Anruf auf dieser Rufnummer registriert, kann er die Verbindung beispielsweise über VoIP an eine gewünschte Auslandsnummer weiterleiten. Um die Callthrough-Funktionalität des Routers zu

4 Mithilfe von UPnP-IGD können Netzwerkgeräte wie IoT selbständig eine Portweiterleitung auf dem Router einrichten.

schützen, sollten sich Anrufer mit einer mindestens 4-stelligen PIN authentisieren. Zudem sollte die Callthrough-Nutzung lediglich für die erforderlichen Anrufernummern aktiviert werden.

5 Virtual Private Network

Ein Virtual Private Network (VPN[5]) wird u. a. verwendet, um aus dem Internet einen verschlüsselten Zugriff auf Daten oder Dienste im internen Netz zu ermöglichen. Sofern eine VPN-Funktionalität vereinzelt benötigt wird, sollte beim Kauf darauf geachtet werden, dass der Router einen VPN-Server bereitstellt. Bei der VPN-Konfiguration des Routers muss für jeden Benutzer ein sicheres Passwort von mindestens 8 Zeichen Länge gesetzt werden. Hierzu bieten diverse Router-Modelle einen Passwortassistenten an, der die Passwortstärke eines Passwortes anzeigt.

6 Management-Informationssystem

Mithilfe eines Management-Informationssystems werden Informationen in Bezug auf den Router zur Verfügung gestellt. Diese Informationen können beispielsweise über die entsprechende Router-App oder über eine im Router hinterlegte E-Mail-Adresse bereitgestellt werden. Ein Management-Informationssystem sollte verwendet werden, um über Änderungen am Router sowie Firmware-Updates informiert zu werden.

7 Konfiguration

Die sichere und zugleich endgültige Konfiguration des Routers sollte gesichert werden, um diese bei Bedarf wieder laden zu können. Zudem sollte sich die Konfigurationsdatei mit einem Passwort schützen lassen.

8 Multi-Faktor-Authentifizierung

Inzwischen besitzen verschiedene Router-Modelle eine Multi- bzw. Zwei-Faktor-Authentifizierung. Mit diesem Verfahren werden u. a. sicherheitskritische Aktionen auf dem Router geschützt, indem die Ausführung beispielsweise durch einen Tastendruck auf dem Router bestätigt werden muss. Eine Zwei-Faktor-Authentifizierung sollte aktiviert werden. Sofern der Router aus dem Internet administriert werden muss und eine Zwei-Faktor-Authentifizierung dies wesentlich erschwert, kann die Zwei-Faktor-Authentifizierung nach einer Abwägung im Einzelfall deaktiviert werden.

9 Kundenbetreuung

Der Router-Hersteller sollte einen technischen Support in Form einer Hotline und eines E-Mail-Supports zur Verfügung stellen. Zudem sollte er auf seiner Webseite oder im Benutzerhandbuch Empfehlungen für eine sichere Konfiguration der Router geben, z. B. durch eine Liste häufig gestellter Fragen (FAQ). Ferner sollte der Hersteller Kontaktdaten für die Meldung von Sicherheitsvorfällen bereitstellen.

10 Weitere Informationen

Zusätzliche Hinweise – insbesondere für Umgebungen mit erhöhtem Schutzbedarf – finden Sie im IT-Grundschutz[6].

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

5 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html
6 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_1_Router_und_Switches.html