Bundesministerium
für Wirtschaft
und Energie

IT-Sicherheit
IN DER WIRTSCHAFT

10 Punkte für einen sicheren Umgang mit Internetroutern in kleinen und mittleren Unternehmen

Ein modernes Unternehmen, gleich welcher Größe und Branche, ist ohne die Nutzung von Informations- und Kommunikationstechnologien kaum noch vorstellbar. Der Auf- und Ausbau sicherer IKT-Systeme ist daher eine unerlässliche Investition in die Zukunft eines jeden Unternehmens.

Das Bundesministerium für Wirtschaft und Energie hat die Initiative „IT-Sicherheit in der Wirtschaft“ eingerichtet. Mit der Initiative sollen vor allem kleine und mittlere Unternehmen für das Thema IT-Sicherheit sensibilisiert und dabei unterstützt werden, ihr IT-Sicherheitsniveau zu verbessern.

Gemeinsam mit IT-Sicherheitsexperten aus Wirtschaft, Wissenschaft und Verwaltung wurden die zehn wichtigsten Punkte für kleine und mittlere Unternehmen zusammengestellt, die keinen professionellen Internetrouter einsetzen:

1. Benennen Sie innerhalb Ihres Unternehmens einen Verantwortlichen für die Wartung, Konfiguration und Zugriffskontrolle des Routers.

2. Halten Sie die Firmware Ihres Routers stets aktuell und überprüfen Sie diese regelmäßig auf neue Herstellerupdates. Abonnieren Sie den Newsletter Ihres Routerherstellers, um zeitnah über kritische Softwareupdates informiert zu werden.

3. Deaktivieren Sie die WPS-Funktion (Wi-Fi Protected Setup) Ihres Routers, da Unbekannte über Sicherheitslücken unautorisierten Zugriff auf Ihren Router erhalten können.

4. Ändern Sie die Standardzugangsdaten zu Ihrem Router und geben Sie Ihrem Router einen langen Benutzernamen sowie ein starkes Passwort, das mindestens 13 Stellen hat und aus Groß-, Kleinbuchstaben sowie Zahlen und Sonderzeichen besteht. Schützen Sie das Passwort vor dem Zugriff unbefugter Personen und ändern Sie es in regelmäßigen Abständen.

5. Deaktivieren Sie den Remote/Fernzugriff auf Ihren Router und öffnen Sie nur die Ports, die unbedingt notwendig sind. Sollte ein Remote/Fernzugriff notwendig sein, dann nutzen Sie in jedem Fall einen verschlüsselten VPN-Zugang.

6. Aktivieren Sie stets Ihre Routerfirewall und überprüfen Sie die Firewallregeln, ggf. auch durch einen IT-Dienstleister.

7. Nutzen Sie die automatische Deaktivierung der Internetverbindung in Ihrem Router bei Inaktivität, z. B. über Nacht. Achten Sie darauf, dass Updates zu dieser Zeit möglichst nicht eingeschränkt werden.

8. Um den Zugang zu Ihrem Router zu erschweren, wählen Sie eine willkürliche SSID für Ihr WLAN, die keinen Rückschluss auf Ihr Unternehmen, Personen oder den eingesetzten Router zulässt. Verschlüsseln Sie Ihr WLAN stets mit den WPA2 Standard und vergeben Sie ein starkes Passwort.

9. Deaktivieren Sie nicht verwendete Funktionen wie beispielsweise UPnP (Universal Plug and Play) an Ihrem Router.

10. Regeln Sie den Zugang zur Ihrem WLAN durch einen MAC-Filter (Media-Access-Control) und definieren Sie so, welche Geräte Zugang zu Ihrem Netzwerk haben.

Weitere Informationen und kostenlose Angebote zum Thema IT-Sicherheit finden Sie auf der Internetseite www.it-sicherheit-in-der-wirtschaft.de.