Sicherheitsmythen entlarvt

RUHR UNIVERSITÄT BOCHUM

RUB

Stabsstelle für Informationssicherheit

Es gibt viele Mythen rund um das Thema IT-Sicherheit, die sich hartnäckig halten. Hier sind einige der größten und häufigsten IT-Sicherheitsmythen:

1. **„Ich bin kein interessantes Ziel."**
   Viele glauben, sie seien für Hacker uninteressant. Tatsächlich befinden sich auf jedem System wertvolle Daten. Opfer automatisierter Angriffe sind häufig ein Türöffner (Patient 0) für Angriffe auf Unternehmensnetzwerke.

2. **„Antivirenprogramme und die Firewall schützen mich vor allen Gefahren."**
   Antivirenprogramme sind wichtig, bieten aber keinen vollständigen Schutz. Viele Angriffe erfolgen über Phishing, Social Engineering oder Sicherheitslücken, die von Antivirenprogrammen nicht erkannt werden. Auch eine Firewall schützt nicht vor Angriffen, die von innen oder über legitime Kanäle erfolgen.

3. **„Starke Passwörter reichen aus."**
   Starke Passwörter sind wichtig, aber nicht ausreichend. Ohne zusätzliche Maßnahmen wie Zwei-Faktor-Authentifizierung (2FA) bleibt das Risiko hoch, vor allem bei Datenlecks. Auch starke Passwörter müssen angemessen geschützt werden. Nutzen Sie z.B. einen Passwortmanager.

4. **„Macs sind immun gegen Viren."**
   Auch Macs und andere Apple-Geräte können Ziel von Malware und Angriffen werden. Die geringere Verbreitung macht sie nur weniger attraktiv für Massenangriffe.

5. **„Updates kann ich aufschieben."**
   Viele glauben, Updates seien lästig und könnten warten. Tatsächlich schließen Updates oft kritische Sicherheitslücken – wer sie aufschiebt, riskiert Angriffe.

6. **„Informationssicherheit ist nur Sache der IT."**
   Sicherheit ist eine Aufgabe für alle Mitarbeitenden. Viele Angriffe zielen auf den „Faktor Mensch" ab, etwa durch Phishing. IT-Sicherheit ist nur ein kleiner Bereich der Informationssicherheit. Technische Maßnahmen allein reichen nicht aus.

7. **„Verschlüsselung macht alles sicher."**
   Verschlüsselung ist wichtig, aber nicht unüberwindbar. Schwache Passwörter, unsichere Schlüsselverwaltung oder Social Engineering können Verschlüsselung aushebeln.

8. **„Sicherheitskopien sind nicht nötig, wenn ich vorsichtig bin."**
   Unfälle, Hardware-Defekte oder Ransomware können jeden treffen. Regelmäßige Backups sind essenziell.

9. **„Der Besuch einer Webseite ist ungefährlich."**
   Beim Besuch einer manipulierten oder kompromittierten Webseite kann Schadsoftware automatisch und unbemerkt auf den Computer heruntergeladen und installiert werden. Webseiten können so gestaltet sein, dass sie vertrauenswürdig wirken und Nutzer dazu verleiten, persönliche Daten, Passwörter oder Kreditkartendaten einzugeben.