Regelmäßige Updates schützen vor Cyberangriffen

8.670 neue Malware-Varianten zählte das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Mai 2022 - ein ganz normaler Monat in der behördlichen Statistik der IT-Bedrohungen. Jeden Monat werden tausende neue Variationen von schädlichen Programmen bekannt. Viele dieser Malware-Varianten nutzen Sicherheitslücken in Betriebssystemen und anderer Software aus und verschaffen Cyberkriminellen Zugriff auf eigentlich geschützte Systeme. Regelmäßige Software-Updates tragen erheblich zum Schutz vor Angriffen bei.

Mit der folgenden Checkliste können Sie für eine sichere Software durch Aktualität sorgen:

- ○ IT-Sicherheit und Updates zur Chefsache machen und auch von Dienstleistern aktiv einfordern.
- ○ Feste Zyklen für die Prüfung auf Software-Updates festlegen.
- ○ Möglichst wenige unterschiedliche Software-Komponenten einsetzen, um den Überblick über Updates zu behalten.
- ○ Mit regelmäßigen Pen-Tests Sicherheitsrisiken identifizieren und beheben.
- ○ Auto-Updates aktivieren, wo immer das möglich ist, ohne die Integrität des Systems und das Zusammenspiel der Komponenten zu gefährden.

Pen-Test:
Der beste Nachweis für die Sicherheit des IT-Systems sind regelmäßige Pen-Tests. „Pen" steht für „Penetration", also das Eindringen ins System. Dabei schlüpfen spezialisierte Dienstleister in die Rolle von Cyberkriminellen. Sie prüfen, wie es Außenstehenden gelingen könnte, in die unternehmenseigenen Systeme einzubrechen und Zugriff auf geschützte Daten zu erlangen. Natürlich geht jedem Pen-Test ein ausführliches Gespräch voraus - der simulierte Angriff wird vorher genau durchgesprochen.

Tipp: Das Bundesamt für Sicherheit in der Informationstechnik hat ein eigenes Zertifikat für Pen-Test-Anbieter entwickelt und listet alle zertifizierten Anbieter auf.