BSI-Lagebericht 2026

Cyber-Bedrohung wächst

[20.11.2026] Die Cyber-Sicherheitslage in Deutschland bleibt angespannt. Laut aktuellem BSI-Lagebericht nutzen Angreifer Sicherheitslücken immer schneller aus. Der Cyber-Sicherheitsrat Deutschland fordert deshalb einen konsequenten Basisschutz und mehr digitale Widerstandsfähigkeit von Unternehmen und Behörden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet die Cyber-Sicherheitslage in Deutschland als „angespannt bis kritisch". Wie aus dem am 19. November veröffentlichten Jahreslagebericht hervorgeht, hat sich insbesondere die Geschwindigkeit von Cyber-Angriffen deutlich erhöht. Im zweiten Quartal 2026 vergingen zwischen dem Bekanntwerden einer Sicherheitslücke und ihrer ersten beobachteten Ausnutzung durchschnittlich nur noch acht Tage. Im vorherigen Berichtszeitraum waren es noch 53 Tage. Gleichzeitig wurden täglich durchschnittlich 160 neue Schwachstellen bekannt – ein Anstieg um 35 Prozent gegenüber dem Vorjahr.

„Cyber-Angriffe werden schneller. Unsere Sicherheitsstrukturen sind es vielerorts noch nicht", warnt Hans-Wilhelm Dünn, Präsident des Cyber-Sicherheitsrat Deutschland Unternehmen und Behörden könnten sich angesichts dieser Entwicklung keine langwierigen Reaktionsprozesse mehr leisten.

Sicherheitsstandards konsequent umsetzen

Die jüngsten Vorfälle verdeutlichen nach Einschätzung des Cyber-Sicherheitsrats die zunehmende Verwundbarkeit digitaler Infrastrukturen. Dazu zählt der bekannt gewordene Cyber-Angriff auf die Europäische Kommission, bei dem mehrere interne Systeme zeitweise beeinträchtigt wurden. Auch die weltweite Störung von Microsoft-365-Diensten in der vergangenen Woche habe gezeigt, welche Folgen die Abhängigkeit von zentralen digitalen Plattformen haben könne. Für einen Cyber-Angriff als Ursache der Microsoft-Störung gibt es bislang allerdings keine belastbaren Hinweise.

Dünn fordert deshalb, grundlegende Sicherheitsmaßnahmen konsequenter umzusetzen. Dazu gehören zeitnahe Sicherheitsupdates, geschützte Zugänge und funktionierende Notfallpläne. Zudem seien risikobasierte Reaktionsfristen für kritische Schwachstellen, regelmäßig überprüfte Sicherheitsstandards und belastbare Wiederanlaufkonzepte notwendig. Insbesondere kleinere Unternehmen und Kommunen müssten dabei stärker unterstützt werden.

Digitale Souveränität stärkt Krisenfestigkeit

Neben dem Schutz vor Angriffen rückt der Cyber-Sicherheitsrat die digitale Souveränität in den Mittelpunkt. Die Konzentration geschäftskritischer Anwendungen auf wenige internationale Plattformen könne systemische Risiken verursachen. „Digitale Souveränität bedeutet nicht, auf internationale Technologie zu verzichten. Sie bedeutet, Abhängigkeiten zu kennen, Alternativen vorzuhalten und auch dann handlungsfähig zu bleiben, wenn zentrale Systeme ausfallen", betont Dünn.

Entscheidend sei daher nicht allein die Einführung zusätzlicher regulatorischer Vorgaben, sondern vor allem die wirksame und überprüfbare Umsetzung bestehender Sicherheitsanforderungen. Cyber-

Sicherheit sei inzwischen eine grundlegende Voraussetzung für eine funktionierende öffentliche Verwaltung, wirtschaftliche Stabilität und staatliche Handlungsfähigkeit.

(al)

BSI-Lagebericht 2026 (PDF)

Stichwörter: IT-Sicherheit, BSI-Lagebericht, Bundesamt für Sicherheit in der Informationstechnik (BSI), Cyber-Sicherheitsrat Deutschland, Cybersicherheit