BSI-Jahreslagebericht

Cybersicherheit bleibt Herausforderung

[12.11.2025] Der neue Jahresbericht des BSI zeigt: Trotz Fortschritten bleibt Deutschland im digitalen Raum verwundbar. Mit der zunehmenden Digitalisierung entstehen auch mehr Schwachstellen, die auch von staatlichen Akteuren ausgenutzt werden. Innenminister Dobrindt setzt beim Schutz auf den geplanten Cyberdome.

Deutschland hat im Bereich der Cybersicherheit Fortschritte erzielt, aber dennoch bleiben digitale Systeme angreifbar. Zu diesem Ergebnis kommt der aktuelle Jahreslagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der jetzt von Bundesinnenminister Alexander Dobrindt und BSI-Präsidentin Claudia Plattner vorgestellt wurde. Demnach sind viele digitale Systeme, Server und Online-Dienste weiterhin unzureichend geschützt und ermöglichen Angreifern, in Netzwerke einzudringen oder Daten zu stehlen. Webanwendungen sind besonders häufig schlecht geschützt, auch Server sind oft falsch konfiguriert und bekannte Sicherheitslücken werden oft zu spät oder gar nicht behoben, so der Bericht.

Jede Schwachstelle wird genutzt

Zwischen Juli 2024 und Juni 2025 ist die Zahl der täglich neu entdeckten Schwachstellen um 24 Prozent gestiegen. Als einen Grund für die Zunahme nennt das BSI die fortschreitende Digitalisierung. Dabei entstehen neue internetbasierte Anwendungen und Systeme – werden diese nicht oder nicht gut genug geschützt, entstehen mögliche Einstiegspunkte für Cyberangriffe. BSI-Präsidentin Claudia Plattner unterstrich, dass jede online erreichbare Institution potenziell bedroht sei. Angreifer suchten gezielt nach Schwachstellen und drängen überall dort ein, wo es möglich ist. Nur wer sich aktiv schütze, könne Risiken verringern und Schäden begrenzen.

Staatlich gesteuerte Akteure zunehmend aktiver

Finanziell motivierte Cyberangriffe gingen laut dem Bericht im Vergleich zum Vorjahr um neun Prozent zurück. Dies wird unter anderem auf erfolgreiche internationale Ermittlungen unter Beteiligung von BKA und BSI zurückgeführt. Trotzdem bleiben Erpressergruppen, die mit Ransomware arbeiten, die größte Bedrohung. Auch staatlich gesteuerte Akteure, die mit komplexen und langfristigen Attacken politische oder wirtschaftliche Ziele verfolgen, sind zunehmend aktiv. Und angesichts globaler Konflikte treten weitere Risiken in den Vordergrund: Besonders im Cloud-Bereich, in der Energieversorgung und in der Fahrzeugindustrie besteht die Gefahr, dass Hersteller oder Anbieter dauerhaft und unkontrolliert Zugriff auf Systeme und Daten behalten. Der Bericht hebt zudem verstärkte Desinformationskampagnen hervor, etwa durch gefälschte oder manipulierte Accounts, vermeintliche Behörden- oder Medienquellen sowie sogenannte Hack-and-Leak-Vorfälle.

Kommunen fehlt Bewusstsein für ihre Gefährdung

Während große Betreiber ihre Schutzmaßnahmen zunehmend ausbauen, fehlen kleineren und mittleren Unternehmen dafür oft die Ressourcen – ebenso wie das Bewusstsein für die eigene Verwundbarkeit. Ähnliche Herausforderungen zeigen sich bei Kommunen, politischen Organisationen, Vereinen und

Parteien. Zur weiteren Verbesserung der Widerstandsfähigkeit im Cyberbereich will das Bundesministerium des Inneren (BMI) den „Cyberdome“ aufbauen, ein teilautomatisiertes System zur Detektion und Analyse von Angriffen sowie zur Reaktion darauf. „Digitale Sicherheit ist eine Kernfrage staatlicher Souveränität. Deshalb geben wir unseren Sicherheitsbehörden die Befugnisse, die sie brauchen, um das Land wirksam zu schützen. Mit dem Cyberdome schaffen wir ein starkes Schild gegen Angriffe aus dem Netz. Der Schutz Deutschlands bleibt eine gemeinsame Aufgabe – von Staat, Wirtschaft und Gesellschaft“, sagte Bundesinnenminister Alexander Dobrindt.

(sib)

Stichwörter: IT-Sicherheit, BSI, Cybersicherheit