ATHENE-Studie

Lücken beim Sicherheitsmonitoring

[17.09.2026] Knapp neun von zehn aktiven IP-Adressen der Bundesverwaltung fehlen laut einer ATHENE-Studie im Monitoring des BSI. Die Forschenden fanden zudem zahlreiche veraltete und kritische Schwachstellen.

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE hat die von außen erreichbare IT der 15 Bundesministerien und des Bundeskanzleramts untersucht. Ein Team unter Leitung von Professorin Haya Schulmann von der Goethe-Universität Frankfurt erfasste dabei auch Systeme bei Dienstleistern und in der Cloud. Die Daten wurden Ende 2025 erhoben.

Insgesamt ordnet ATHENE der Bundesverwaltung rund 36.100 aktive IP-Adressen zu. Im Monitoring des Bundesamts für Sicherheit in der Informationstechnik (BSI) seien dagegen nur rund 3.800 enthalten. Mehr als 60 Prozent der erfassten Adressen würden inzwischen extern oder in der Cloud betrieben. In den nicht vom BSI-Monitoring erfassten Bereichen stellte ATHENE mehr als 12.100 Sicherheitsbefunde fest.

Tausende bekannte Schwachstellen

Auch bei grundlegenden Sicherheitsmaßnahmen sieht die Studie Defizite. 32,5 Prozent der untersuchten Zertifikate seien fehlerhaft oder abgelaufen, 45 Prozent der Mail-Domänen nicht wirksam gegen gefälschte Absender geschützt. Kein untersuchtes Ministerium erfülle die einschlägigen BSI-Vorgaben durchgängig.

#INFO#Insgesamt zählt ATHENE 15.290 Fundstellen für bekannte Schwachstellen (CVE). Ihr Durchschnittsalter beträgt 7,6 Jahre. Von mehr als 2.182 kritischen Schwachstellen stammen 1.050 aus den Jahren 2015 bis 2017. In elf Ministerien sei außerdem noch PHP 5 im Einsatz, dessen Hersteller-Support Ende 2018 ausgelaufen ist.

Eine Herausforderung ist laut Studie die dezentrale IT-Landschaft des Bundes. Große Teile der extern erreichbaren Infrastruktur werden von nachgeordneten Behörden und Dienstleistern betrieben. Bei den untersuchten Beispielen BMI, BMAS und BMF entfielen 88 bis 93 Prozent der sichtbaren Hosts auf die jeweiligen Geschäftsbereiche und deren Dienstleister.

Vollständiges IT-Register gefordert

ATHENE empfiehlt deshalb ein extern validiertes Register aller IT-Ressourcen des Bundes, das auch Cloud-Dienste, nachgeordnete Behörden und Dienstleister berücksichtigt. Zudem sollten überprüfbare Sicherheitsanforderungen in Betreiber- und Beschaffungsverträgen verankert und verbindliche Termine für die Abschaltung von Altsystemen festgelegt werden. „Sicherheit entscheidet sich nicht an neuen Plattformen, sondern an Grundhygiene, an verbindlichen Vorgaben in Betreiberverträgen und an der Bereitschaft, Altsysteme tatsächlich abzuschalten“, sagt Studienleiterin Schulmann.

(al)

ATHENE-Studie „IT der Bundesministerien 2025 – Kernergebnisse und Handlungsempfehlungen“

Stichwörter: IT-Sicherheit, ATHENE, Cyber Security