NACHRICHTEN AG

08. Mai 2025

Massiver Cyberangriff auf Stuttgart: Politiker fordern sofortige Maßnahmen!

FDP und SPD fordern nach DDoS-Angriff auf Stuttgart mehr Cybersicherheitsinvestitionen in Baden-Württemberg. CSBW bleibt zentral.

Stuttgart, Deutschland - In Baden-Württemberg nehmen die Rufe nach einer Stärkung der Cybersicherheit zu, insbesondere nach einem jüngsten Cyberangriff auf die Stadt Stuttgart. Die FDP und die SPD haben sich in der Debatte um Sicherheitsmaßnahmen lautstark geäußert und fordern höhere Investitionen in die IT-Sicherheit. Die aktuelle Lage wird vom Innenministerium als angespannt bezeichnet, da DDoS-Angriffe (Distributed Denial of Service) zunehmend zu einem Problem werden. Diese Art von Angriffen, wie der auf stuttgart.de am 30. April, zeigt die Verwundbarkeit öffentlicher Institutionen.

Der Cyberangriff, der von der prorussischen Hackergruppe **NoName057(16)** verübt wurde, sorgte dafür, dass die Bürger

die Webseite der Stadt für einige Zeit nicht erreichen konnten und es zu Fehlermeldungen kam. Die Attacke, die auch andere deutsche Städte wie Berlin und Nürnberg betroffen hat, richtete sich gezielt gegen die Internetpräsenz der Stadt Stuttgart und begann am 29. April nachmittags.

Reaktionen und Forderungen der Politik

In der politischen Diskussion betont Jonas Hoffmann von der SPD die Notwendigkeit eines geschulten Personals sowie der Implementierung technischer Maßnahmen wie Firewalls und einem effektiven Patchmanagement. Zudem fordert die FDP unter Leitung von Daniel Karrais eine Trendwende in der IT-Sicherheitspolitik und gemeinsame Standards mit Kommunen. Dies beinhaltet auch die Durchführung eines umfassenden Cybersicherheitschecks aller IT-Strukturen.

Die Cybersicherheitsagentur Baden-Württemberg (CSBW), die seit dem 1. Januar 2022 aktiv ist, wurde bereits vor dem Angriff aktiviert und hatte die Stadtverwaltung Stuttgart über die drohende Gefahr informiert. Die zentrale Aufgabe der CSBW ist die Förderung der Cybersicherheit, insbesondere für öffentliche Stellen. Sie bietet nicht nur Cyber-Ersthilfe, sondern auch Schulungen für die Mitarbeiter der Behörden an, um sie auf zukünftige Bedrohungen besser vorzubereiten.

Übergreifende Cyberbedrohungen in Deutschland

Der aktuelle Bericht des **Bundesamts für Sicherheit in der Informationstechnik (BSI)** beschreibt die Cybersicherheitslage in Deutschland als besorgniserregend. Cyberkriminelle professionalisieren ihre Techniken und nutzen moderne Technologien. Besonders hervorzuheben ist die Zunahme hochvolumiger DDoS-Angriffe und Ransomware-Vorfälle, die kleine bis mittlere Unternehmen sowie Kommunen stark belasten.

Die Digitalisierung, so der BSI-Bericht, trägt zur Vergrößerung der Angriffsflächen bei, was die IT-Sicherheit besonders herausfordernd macht. Die Sicherheitslage wird nicht nur durch externe Bedrohungen, sondern auch durch interne Schwachstellen, etwa in Perimetersystemen, gefährdet. Die Notwendigkeit eines nachhaltigen Ansatzes zur Verbesserung der Cybersicherheit wird deutlich: Sicherheit muss durch Kooperation aller Beteiligten in Wirtschaft, Wissenschaft und Politik gewährleistet werden.

Stuttgart kann sich auf die CSBW stützen, um die IT-Infrastruktur zu sichern. Die Stadt hat bereits erste Maßnahmen zur Stärkung der IT-Security eingeleitet und prüft weitere Schritte. Details zu diesen Maßnahmen bleiben jedoch aus Sicherheitsgründen geheim. Dennoch ist klar, dass die jüngsten Ereignisse die Dringlichkeit unterstreichen, mehr in die Cybersicherheit zu investieren und die Resilienz gegen zukünftige Angriffe zu erhöhen.

Details	
Vorfall	Cyberkriminalität
Ursache	DDoS-Angriff
Ort	Stuttgart, Deutschland
Quellen	• **www.swr.de** • **www.stuttgarter-nachrichten.de** • **www.bsi.bund.de**