Baden-Württemberg unter Cyberangriff: Alarmstufe Rot für Unternehmen!

Baden-Württemberg sieht sich täglichen Cyberangriffen aus Russland gegenüber; Maßnahmen zur Verteidigung und Sicherheit werden diskutiert.

Stuttgart, Deutschland - In Baden-Württemberg sind die Behörden alarmiert angesichts der wachsenden Zahl von Cyberattacken, die zunehmend als Teil eines hybriden Kriegs gegen Deutschland betrachtet werden. Laut dem SWR wird der Landeskommandant der Bundeswehr, Kapitän zur See Michael Giss, immer besorgter über die Zunahme dieser Angriffe, die teilweise auf russische Akteure zurückzuführen sind. Täglich sind die Landesbehörden in Baden-Württemberg rund 1.000 Mal Ziel solcher Attacken, wobei sowohl kriminelle als auch staatliche Akteure hinter den Angriffen vermutet werden.

Besonders gefährdet sind Unternehmen aus der Auto-, Logistik- und Rüstungsindustrie, die laut Giss als strategische Ziele für

mögliche Feinde gelten. Der anhaltende russische Angriffskrieg auf die Ukraine hat die Verteidigungsbemühungen in Deutschland verstärkt. Um dieser Bedrohung wirksam zu begegnen, berät die Landesregierung von Baden-Württemberg mit Vertretern aus der Forschung, Rüstungs- und IT-Branche über Sicherheitsmaßnahmen und Strategien zur Verteidigung.

Hybride Bedrohungen und ihre Folgen

Die Bundeswehr plant, sich verstärkt auf hybride Bedrohungen einzustellen. Dazu gehören auch unautorisierte Drohnenflüge über Bundeswehrstandorte, die zunehmend beobachtet werden. Giss warnt vor sogenannten ȣWegwerfagentenȣ, die für Spionagezwecke eingesetzt werden und Informationen über die Infrastruktur der Bundeswehr sammeln. Diese Aktivitäten könnten Teil einer Strategie sein, die darauf abzielt, die Gesellschaft zu destabilisieren, bevor ein offener militärischer Konflikt entsteht, so Security Insider.

Zusätzlich zu Cyberangriffen berichten deutsche Unternehmen von vermehrten Spionageversuchen aus China, während die Bundesregierung zu den Angriffen aus Russland vage Stellung nimmt. Die permanente Bedrohung führt zu einem gesteigerten Bewusstsein für die Sicherheitslage, wobei das Landesamt für Verfassungsschutz von einer erhöhten Gefährdung durch Sabotageaktivitäten spricht. Innenminister Thomas Strobl hebt die Notwendigkeit hervor, die zivile Verteidigung zu stärken und die Bundeswehr hierbei zu unterstützen.

Schutzmaßnahmen und strategische Antworten

Um dem hybriden Krieg zu begegnen, hat Baden-Württemberg verschiedene Bedrohungsszenarien entwickelt und plant, einen Runden Tisch einzuberufen, um Schutzmaßnahmen für betroffene Unternehmen zu diskutieren. Ministerpräsident Winfried Kretschmann sieht in der Rüstungsindustrie einen

wirtschaftlichen Impuls und strebt eine Technologieführerschaft im Defense-Bereich an. Der geplante Ausbau der Rüstungsindustrie in Baden-Württemberg soll es der Region ermöglichen, von den anstehenden Milliardeninvestitionen in Europas Militär zu profitieren, wie der BR berichtet.

Hinsichtlich der Cyberangriffe wird immer wieder auf die Schwierigkeiten hingewiesen, diese rechtzeitig zu erkennen und entsprechend darauf zu reagieren. Die Bundesregierung hat Maßnahmen zur Prävention und Detektion zugesagt, bleibt jedoch in den Antworten auf konkrete Anfragen oft vage.

Mit der zunehmenden Gefahr durch hybride Bedrohungen wird auch der Ruf nach neuen gesetzlichen Regelungen lauter, um der Bundeswehr mehr Handlungsspielraum zu geben. Ein aktueller Gesetzentwurf sieht vor, dass die Bundeswehr unter bestimmten Bedingungen Drohnen, die unbefugt über militärische Einrichtungen fliegen, zur Not auch abschießen darf.

Details	
Vorfall	Cyberkriminalität
Ort	Stuttgart, Deutschland
Quellen	• www.swr.de • www.security-insider.de • www.br.de