NACHRICHTEN AG

08. April 2025

Russische Hackerattacke: DGO im Visier – Sicherheitslage alarmierend!

Russische Hackerangriffe auf die Deutsche Gesellschaft für Osteuropakunde: Analyse durch BSI und Verfassungsschutz. Cybersicherheit in Gefahr.

Berlin, Deutschland - Am 8. April 2025 wurde bekannt, dass die Deutsche Gesellschaft für Osteuropakunde (DGO) Ziel eines mutmaßlichen russischen Cyberangriffs war. Laut Informationen von **ZVW** wird dieser Angriff der Hackergruppe APT 29, auch bekannt als „Cozy Bear“, zugeschrieben. Diese Gruppe wird mit dem russischen Geheimdienst SWR in Verbindung gebracht. Die DGO hatte Ende März 2025 nach einem unautorisierten Zugriff auf ihren Mailserver die Situation öffentlich gemacht.

Der Zugriff auf die Systeme der DGO wurde durch eine IP-Adresse möglich, die bereits in einem ähnlichen Angriff im Jahr zuvor verwendet wurde. Der Vorfall zeigt, wie anfällig Organisationen sind, insbesondere wenn sie sich mit Themen rund um Russland und Belarus beschäftigen. Andere Organisationen in Berlin berichteten ebenfalls von physischen Nachstellungen und Einbrüchen.

Warnungen und Sicherheitsmaßnahmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie das Bundesamt für Verfassungsschutz sind in die Analyse des Vorfalls involviert. Im Zuge dessen hat der Verfassungsschutz ein Warnschreiben an rund 70 wissenschaftliche Einrichtungen und Vereine verschickt, um auf die Bedrohung durch russische Cyberangriffe hinzuweisen. Diese

Warnungen sind besonders relevant, da die DGO seit Februar 2024 in Russland als „unerwünscht“ eingestuft wurde und seit Juli 2024 als „extremistisch“ gilt. Dies bedeutet, dass die DGO in Russland nicht mehr aktiv sein kann und Kooperationen mit ihr für russische Experten strafbar sind.

Die DGO hat nach dem ersten Vorfall ihre IT-Sicherheit erhöht, sieht sich jedoch aufgrund begrenzter personeller Ressourcen Herausforderungen gegenüber. Die fortschreitende Professionalisierung der Cyberkriminalität macht es für Organisationen noch schwieriger, sich gegen angreifende Hacker zu verteidigen.

Die aktuelle Cyberlage in Deutschland

Diese Entwicklungen spiegeln die besorgniserregende IT-Sicherheitslage in Deutschland wider, wie im Lagebericht des BSI aus dem Jahr 2024 erwähnt wird. Der Bericht analysiert die Cyberlage in fünf Dimensionen, darunter Bedrohung, Angriffsfläche und Resilienz. Die Cybersicherheitsbehörde des Bundes hebt hervor, dass Cyberkriminelle zunehmend moderne Technologien nutzen und strukturierte Dienstleistungen im Cyberraum anbieten. Letzteres verschärft die Risiken für Unternehmen und Institutionen in Deutschland.

Darüber hinaus wurden in letzter Zeit viele deutsche politische Stiftungen sowie andere Institutionen als „unerwünscht“ in Russland eingestuft. Diese Entwicklung erfolgt im Kontext des Ukraine-Kriegs und zeigt die wachsenden Spannungen und Herausforderungen auf, mit denen Organisationen konfrontiert sind.

Die Zunahme von Ransomware-Angriffen, die häufig kleine und mittlere Unternehmen sowie Kommunen betreffen, ist ein weiteres alarmierendes Zeichen. Im ersten Halbjahr 2024 erlebte Deutschland einen signifikanten Anstieg hochvolumiger DDoS-Angriffe. Zudem wird geschätzt, dass weltweit über 1,1 Milliarden US-Dollar durch Ransomware-Angriffe erbeutet

wurden, wobei die Dunkelziffer noch höher sein könnte.

Um diesen Bedrohungen zu begegnen, hat Deutschland in den letzten Jahren umfassende Fortschritte in Richtung einer resilienten Cybernation gemacht. Es besteht jedoch weiterhin ein dringender Bedarf an der Zusammenarbeit aller Beteiligten, einschließlich Herstellern und Verbrauchern, um die Cybersicherheitsstandards zu erhöhen und sicherere Produkte zu entwickeln. Der BSI-Bericht wird ab 2025 nicht mehr gedruckt, sondern ausschließlich online zur Verfügung stehen, was den digitalen Wandel im Bereich der Cybersicherheit unterstreicht.

Details	
Vorfall	Cyberkriminalität
Ort	Berlin, Deutschland
Quellen	• **www.zvw.de** • **www.bsi.bund.de**