Presse

Niedersachsen

Niedersächsisches Ministerium für
Inneres, Sport und Digitalisierung

17.11.2025

Wirtschaftsschutz in Zeiten hybrider Bedrohungen: Knapp 400 Vertreterinnen und Vertreter aus der Wirtschaft haben sich ein umfassendes Bild zu aktuellen Sicherheitsthemen verschafft

Behrens: „Die Bundesregierung und die niedersächsische Landesregierung sind sich der erhöhten Risiken bewusst und verstärken ihre Sicherheitsmaßnahmen nachhaltig“

Auf der 24. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes hat die Niedersächsische Ministerin für Inneres, Sport und Digitalisierung, Daniela Behrens, die allgemeine Sicherheitslage erläutert und Schutzmöglichkeiten gegen hybride Bedrohungen aufgezeigt. An der heutigen Tagung in Hannover haben knapp 400 Vertreterinnen und Vertreter aus verschiedenen Wirtschaftszweigen teilgenommen und die Gelegenheit genutzt, sich in gezielten Impulsvorträgen ein umfassendes Bild zu aktuellen Sicherheitsthemen zu verschaffen und sich direkt mit Sicherheitsbehörden des Bundes und der Länder auszutauschen. Zu den Vortragenden gehörte auch die Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Claudia Plattner.

Hybride Bedrohungen haben viele Erscheinungsformen, mit denen fremde Staaten versuchen, durch verdeckte Aktionen auf Politik und Gesellschaft eines anderen Landes Einfluss zu nehmen. Dazu gehören klassische Spionageaktivitäten, aber auch das Verbreiten von Desinformationskampagnen, Cyberangriffe oder Sabotageakte bzw. deren Vorbereitung wie z. B. das Auskundschaften von Kritischer Infrastruktur. Das Ziel solcher Maßnahmen ist es, unter anderem nationale Interessen zu schwächen – sei es durch das Unterminieren demokratischer Institutionen, die Zerstörung sozialer Strukturen oder die Schädigung von Wirtschafts- oder Technologiebereichen und militärischen Sektoren.

Nr. 098/2025		
Pressestelle	Tel.: (0511) 120-6259	www.mi.niedersachsen.de
Schiffgraben 12, 30159 Hannover	Fax: (0511) 120-99-6555	E-Mail: pressestelle@mi.niedersachsen.de

Ministerin Behrens: „Der russische Angriffskrieg gegen die Ukraine führt nicht nur zu geopolitischen Spannungen und einem Paradigmenwechsel in der Verteidigungspolitik, sondern auch zu Veränderungen in der Wirtschaft. Für andere Staaten ist Deutschland wegen seiner Innovations- und Wirtschaftskraft sowie seiner zentralen geografischen Lage von besonderem Interesse. Die Bundesregierung und die niedersächsische Landesregierung sind sich der erhöhten Risiken bewusst und verstärken daher ihre Sicherheitsmaßnahmen nachhaltig, vor allem im Bereich der Kritischen Infrastruktur. So sind zum Beispiel Polizei und Verfassungsschutz aktiv in die Sicherheitsüberprüfung von Personen eingebunden, die in sensiblen Bereichen arbeiten. Das reduziert das Risiko von Sabotageaktionen. Die neue Sicherheitsstrategie der Bundesregierung zielt zudem darauf ab, die Rüstungsindustrie zu stärken und in die Cybersicherheit sowie in sicherheitsrelevante Technologien zu investieren. Niedersachsen, als Standort wichtiger Unternehmen und logistische Drehscheibe, spielt dabei eine zentrale Rolle. Unsere staatlichen Behörden arbeiten daher auch ganz praktisch mit den Wirtschaftsunternehmen zusammen, indem sie zum Beispiel im Bereich der Cybersicherheit Schulungen zum Schutz vor Hackerangriffen anbieten.“

Angriffe wie das Auskundschaften von Kritischer Infrastruktur sind oft schwer als solche zu identifizieren, da sie in der Regel gezielt verübt werden, wobei die staatliche Urheberschaft verschleiert wird. Sie werden daher oft nicht direkt als Bedrohung wahrgenommen. Dieses Vorgehen stellt Sicherheitsbehörden vor erhebliche Herausforderungen, insbesondere bei der richtigen Einschätzung und Einordnung konkreter Vorfälle und potenzieller hybrider Gefahren.

Der Niedersächsische Verfassungsschutzpräsident Dirk Pejril sagt dazu: „Niedersachsen hat in den vergangenen Jahren wichtige Grundlagen geschaffen, um das Zusammenspiel aus Vernetzung und Sensibilisierung voranzutreiben. Der Single Point of Contact (SPoC Hybrid) beim Verfassungsschutz bündelt schnell und umfangreich Informationen zu hybriden Bedrohungen und initiiert präventive Maßnahmen der Landesverwaltung, der Sicherheitsbehörden, auf kommunaler Ebene und vor allem in den Unternehmen.“

BSI-Präsidentin Claudia Plattner erklärt: „Deutschland ist weiterhin ein attraktives Ziel für Cyberangriffe. Spionage, Sabotage und Kriminalität aus dem Cyberraum bedrohen nicht nur unsere Wirtschaftskraft, sondern auch unsere Demokratie. Wir müssen die Cybernation Deutschland weiter ausbauen und uns klarmachen: Jede aus dem Internet erreichbare Institution oder Person ist prinzipiell durch Cyberangriffe bedroht. Angreifer suchen gezielt nach den verwundbarsten Angriffsflächen. Mit dem jüngst verabschiedeten Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie hat Deutschland einen wichtigen Meilenstein auf dem Weg zu einer resilienten Cybernation erreicht, denn wir schützen damit einen entscheidenden Teil unserer digitalen Angriffsfläche viel besser als bisher."

Cyberoperationen im öffentlichen und privaten Sektor bedrohen kontinuierlich die Leistungs- und Funktionsfähigkeit von Unternehmen und kritischen Anlagen. Sie verursachen nicht nur erhebliche finanzielle Schäden, sondern verlangen auch eine fortwährende Stärkung der Abwehrkapazitäten. Dabei geraten nicht nur Großunternehmen und Betreiber Kritischer Infrastrukturen ins Visier, sondern auch der breite Mittelstand, der das Rückgrat der Wirtschaft, insbesondere in Niedersachsen, bildet.