**Keynote**

der Ministerin für Inneres, Sport und Digitalisierung,

Daniela Behrens,

**24. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes**

am 17. November 2025, 13.00 Uhr

---

Zeitansatz: ca. 12 – 15 min.

**Es gilt das gesprochene Wort!**

## Begrüßung und Einführung

Sehr geehrte Damen und Herren,
sehr geehrte Referentinnen und Referenten,
liebe Kolleginnen und Kollegen,
liebe Gäste,

auch ich möchte Sie ganz herzlich zur 24. Wirtschaftsschutztagung 2025 hier in Hannover begrüßen – ausgerichtet durch den niedersächsischen Verfassungsschutz.

Mein herzlicher Dank gilt daher Ihnen, Herr Pejril, und all Ihren Mitarbeiterinnen und Mitarbeitern, die diese Tagung wieder einmal möglich gemacht haben!

Was einst mit kleinen, vertraulichen Gesprächskreisen begann, ist heute eine feste Größe in der Sicherheitsarchitektur unseres Landes – eher schon eine Institution. Nicht nur die 400 Gäste, sondern auch die hochkarätige Besetzung der einzelnen Programmpunkte sprechen da für sich.

Ich erachte es als höchst wertvoll, dass wir hier zusammenkommen, um Erfahrungen auszutauschen, Handlungsstrategien zu diskutieren und die Zusammenarbeit zwischen Staat und Wirtschaft weiter zu stärken. Nur so können wir die aktuellen Herausforderungen meistern.

Somit gilt mein Dank auch Ihnen, liebe Gäste, dass Sie bereit sind, sich mit den drängenden Themen, die uns alle beschäftigen und bewegen, auseinanderzusetzen.

## *Hybride Bedrohungen – aktuelle Entwicklungen*

Sehr geehrte Damen und Herren,

unsere Sicherheitslage hat sich in den letzten Jahren spürbar verändert. Hybride Bedrohungen sind keine Randerscheinung mehr, sondern Teil unseres Alltags.

Gezielte Desinformation, Cyberangriffe, Spionage und Sabotage – sie alle zielen darauf ab, Vertrauen zu untergraben, Entscheidungsprozesse zu stören und wirtschaftliche Stabilität zu gefährden.

BND-Präsident Martin Jäger hat es kürzlich auf den Punkt gebracht:

> „*Das Handeln Russlands ist darauf angelegt, die NATO zu unterminieren, europäische Demokratien zu destabilisieren und unsere Gesellschaften zu spalten*."

Diese Einschätzung teilt auch unser Lagebild in Niedersachsen.

Wir müssen davon ausgehen, dass staatliche und nichtstaatliche Akteure hybride Mittel einsetzen – oft verdeckt, schleichend und über längere Zeiträume. Das verlangt Wachsamkeit und Zusammenarbeit zwischen Sicherheitsbehörden, Wirtschaft und der Zivilgesellschaft.

Nach einer aktuellen Bitkom-Studie waren 87 Prozent aller Unternehmen in Deutschland Ziel von Cyberangriffen, Spionage oder Sabotage. Der Schaden: rund 289 Milliarden Euro pro Jahr.

Die Summe zeigt eindrücklich, wie gravierend wirtschaftliche Sicherheitsrisiken inzwischen geworden sind – und das Wirtschaftsschutz längst nicht mehr nur Großunternehmen betrifft, sondern alle Betriebe aller Branchen und Größen.

Gerade Niedersachsen ist mit seiner starken Industrie, seinen Forschungsstandorten und seinem innovationsstarken Mittelstand besonders im Fokus internationaler Akteure.

Die zunehmende Digitalisierung macht uns produktiver – aber eben auch verwundbarer.

Wie konkret diese Gefahr ist, zeigt auch ein aktuelles Beispiel aus Baden-Württemberg:

Ende August wurde die Arbeiterwohlfahrt Karlsruhe-Land Opfer eines massiven Cyberangriffs. Eine Ransomware legte das gesamte IT-System lahm.

Die Arbeitsfähigkeit war tagelang stark eingeschränkt.

Erst durch das Zusammenspiel von Landeskriminalamt, Datenschutzbehörden und externen Fachleuten gelang es, die Lage unter Kontrolle zu bringen. Dabei konnte die Schadsoftware einem russischen Hacker-Netzwerk zugeordnet werden.

Dieses Beispiel steht stellvertretend für viele.

Auch in Niedersachsen sind wir nicht davor gefeit.

Niedersächsische Unternehmen waren jüngst Ziel internationaler Angriffe, teils mit erheblichen Folgen für den laufenden Betrieb.

So gab es zuletzt auch Verdachtsmomente, wonach staatliche Akteure an Cyberangriffen auf Unternehmen der Kritischen Infrastruktur (KRITIS) beteiligt sind.

Diese besonders sensiblen Einrichtungen der Daseinsvorsorge sind dank diverser gesetzlicher Vorgaben grundsätzlich gut vor Cyberangriffen geschützt.

Jedoch zeigt die Erfahrung, dass es auch im digitalen Raum kaum gelingen kann, eine hundertprozentige Sicherheit zu gewährleisten.

Zunehmend beobachten wir außerdem neue Angriffsmuster:

- KI-gestützte Phishing-Versuche,
- Identitätsdiebstahl über manipulierte Social-Media-Konten
- und die gezielte Nutzung von Smart-Home-Geräten oder Cloud-Zugängen.

All dies zeigt, wie sehr digitale Risiken in unseren Alltag vorgedrungen sind – in Unternehmen ebenso wie in private Lebensbereiche.

Und der Bereich der Cybersicherheit selbst wird zunehmend Teil hybrider Auseinandersetzungen.

So werden einfache Hacker oder Datenhändler als sogenannte „Low-Level-Agenten“ für einfache Phishing-Angriffe und das Einschleusen von Schadsoftware eingesetzt - und das oft ohne Wissen über das eigentliche dahinterstehende Ziel der Auftraggeber.

Dieser indirekte Modus Operandi ermöglicht es fremden Nachrichtendiensten, im Zielland zu operieren, ohne Spuren klassischer Agententätigkeit zu hinterlassen.

Das verdeutlicht: Jeder ungesicherte Zugang kann zur Schwachstelle werden.

## *Wie Niedersachsen reagiert – strategischer Rahmen und Initiativen*

Meine sehr geehrten Damen und Herren,

wir als Landesregierung haben den Anspruch, den strategischen Rahmen zu schaffen, damit Sie handlungsfähig bleiben.

Klar ist dabei aber auch, dass es zur Stärkung der Cybersicherheit ein Zusammenwirken vieler Akteure braucht.

Deshalb stärken wir die Cybersicherheit in Niedersachsen auf mehreren Ebenen:

- durch neue Initiativen für hybride Bedrohungen,
- durch zentrale Ansprechstellen beim Verfassungsschutz,
- und durch eine noch engere Vernetzung zwischen Staat, Wirtschaft und Wissenschaft.

Wir wollen, dass Unternehmen nicht nur reagieren, sondern selbst aktiv ihre eigene Widerstandskraft stärken können - durch Sensibilisierung, Mitarbeiterschulungen, klar definierte Notfallpläne und gelebter Sicherheitskultur.

Der Schutz beginnt dort, wo Ihr Wissen und Ihre Erfahrung täglich wirken: in der IT, in der Unternehmensführung, in der Verantwortung gegenüber Ihren Beschäftigten.

Unser gemeinsames Ziel muss sein, die immer professionelleren und automatisierten Angriffe abzuwehren und auch kleine Unternehmen mit modernen Sicherheitskonzepten zu unterstützen.

Ein vernetztes Zusammenwirken spielt jedoch nicht ausschließlich im Bereich der Cybersicherheit eine gewichtige Rolle.

Die aktuellen geopolitischen Entwicklungen adressieren weitere neue Verantwortungen an politische Akteure und unsere Sicherheitsbehörden.

Die Bundeswehr stellt sich aktuell im Rahmen des Operationsplan Deutschland (OPLAN) auf Szenarien ein, von denen wir gehofft hätten, dass sie in unserer Lebensrealität in Europa keine Rolle mehr spielen würden.

Ich sage aber auch klar: Wir können und dürfen die Gefahr, die vom russischen Aggressor ausgeht, nicht ignorieren und wir müssen akzeptieren, dass Frieden keine Selbstverständlichkeit ist.

Deshalb halte ich es für gut und richtig, sich konzeptionell auf mögliche Szenarien vorzubereiten, die uns erwarten könnten, sollten die militärischen Auseinandersetzungen noch näher an unser Land heranrücken.

Es wird hier entscheidend darauf ankommen, dass der Bund die Länderverantwortlichen umfassend in die Konzeptionen einbezieht.

Parallel dazu haben wir aber auch in Niedersachsen begonnen, die Vernetzung zwischen Sicherheitsbehörden, militärischen Vertretern und zivilgesellschaftlichen Akteuren zu intensivieren. Wir müssen Themen der Inneren und Äußeren Sicherheit viel stärker als bisher gemeinsam denken.

Der durch den Ministerpräsidenten Anfang September ins Leben gerufene Sicherheitspolitische Dialog bietet dabei ein gutes Forum, um die verschiedenen Facetten der absolut notwendigen gedanklichen Vorplanungen zu bündeln.

Ziel ist es, durch eine engere Verzahnung bestehender Konzepte und Strategien die zivile Verteidigung und unsere gesellschaftliche Resilienz noch besser aufzustellen.

Auch Vertreterinnen und Vertreter der Wirtschaft waren bei der Auftaktveranstaltung zugegen und sollen im weiteren Prozess eingebunden werden.

## *Abschluss*

Meine Damen und Herren,

Wirtschaftsschutz ist heute mehr denn je ein Innovationsmotor.

Wer Sicherheit denkt, stärkt Wettbewerbsfähigkeit, Vertrauen und Zukunftsfähigkeit.

Niedersachsen will dabei Partner und Impulsgeber sein – nicht Kontrolleur. Mit jeder Schulung, jeder Kooperation, jedem Dialog wächst unser gemeinsames Sicherheitsnetz.

Die Wirtschaftsschutztagung selbst ist Teil dieser Präventionsarbeit.

Nutzen Sie den heutigen Tag, um Kontakte zu vertiefen, Erfahrungen zu teilen und neue Impulse mitzunehmen.

Fungieren Sie als Multiplikatorinnen und Multiplikatoren – in Ihre Unternehmen, Ihre Netzwerke und Ihre Regionen hinein.

Wir müssen die Stärkung der Cybersicherheit weiter vorantreiben. In diesem Zusammenhang freue mich ganz besonders, dass die Präsidentin des Bundesamtes für Informationssicherheit (BSI) diese Tagung unterstützt und uns gleich noch ausführlichere Einblicke in diese Thematik bieten wird. Vielen Dank für Ihren Besuch und Ihre Unterstützung, Frau Plattner!

Herzlichen Dank für Ihre Aufmerksamkeit, Ihr Engagement, Ihre Expertise und Ihre Bereitschaft zum Dialog. Gemeinsam gestalten wir die Zukunft sicher, resilient und innovativ.