LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/244**
8. Wahlperiode **12.01.2022**

ANTRAG

der Fraktion der CDU

IT-Sicherheit unserer Wirtschaft verbessern - kleine und mittlere Unternehmen schützen

Der Landtag möge beschließen:

I. Der Landtag stellt fest:

Cyberkriminalität stellt eine wachsende Bedrohung für Unternehmen in unserem Land dar. Besonders kleine und mittlere Unternehmen stehen vor der Herausforderung, ein umfassendes Bewusstsein für diese Bedrohung zu entwickeln sowie das notwendige Know-how und ausreichend Ressourcen für die Gefahrenabwehr bereitzustellen. Da diese Unternehmen einen Großteil der Arbeitsplätze in Mecklenburg-Vorpommern stellen und einen wesentlichen Beitrag zur Innovationsfähigkeit leisten, liegt in deren Cybersicherheit ein wesentliches Zukunftsinteresse unseres Landes.

II. Die Landesregierung wird aufgefordert,

1. gemeinsam mit den Industrie- und Handelskammern, Unternehmerverbänden, den Handwerkskammern sowie IT-Sicherheitsexperten einen Dialog- und Vernetzungsprozess zu initiieren mit dem Ziel, das Bewusstsein für das Thema Cybersicherheit in der internen Kommunikation der Verbände an die Mitgliedsunternehmen zu stärken und Maßnahmen für die Verbesserung der IT-Sicherheit von kleinen und mittleren Unternehmen in Mecklenburg-Vorpommern zu generieren. So sollten beispielsweise grundlegende Handlungsempfehlungen zur Verbesserung der IT-Sicherheit sowie dem Umgang bei Cyberangriffen entwickelt und bekannt gemacht werden. Dafür wird die Landesregierung auch die Netzwerke der Innovationszentren in Mecklenburg-Vorpommern und das Know-how des Computer-Notfall-Teams (Computer Emergency Response Team, kurz CERT) Mecklenburg-Vorpommerns nutzen.

2. dem Thema Cybersicherheit in der Wirtschaftsförderung des Landes mehr Bedeutung einzuräumen und für das Ziel, vermehrt Investitionen der kleinen und mittleren Unternehmen in Datenschutz und IT-Sicherheit zu fördern, die Mittel für die Förderung der Investitionen für digitale Transformation gemäß DigiTrans-Richtlinie Mecklenburg-Vorpommern auf jährlich zehn Millionen Euro aufzustocken. Diese Förderung ist in den Folgejahren entsprechend zu verstetigen und im Doppelhaushalt 2022/2023 sowie der Mittelfristigen Finanzplanung einzustellen. Um neben der Digitalisierung von Geschäftsprozessen die Förderung der IT-Sicherheit als separaten Zuwendungszweck der Richtlinie (Nummer 1.1 Buchstabe b) maßgeblich auszuweiten, ist die Hälfte des Budgets von zehn Millionen Euro ausschließlich für diesen Zuwendungszweck vorzusehen.
3. alle vorhandenen Fördermöglichkeiten des Landes und auch des Bundes für Unternehmensinvestitionen von kleinen und mittleren Unternehmen in IT-Sicherheit durch Informationskampagnen bekannter zu machen und jährlich zu evaluieren, ob diese Fördermaßnahmen auch verstärkt für das Ziel einer Erhöhung der IT-Sicherheit durch die kleinen und mittleren Unternehmen in Mecklenburg-Vorpommern genutzt werden.
4. den zuständigen Ausschuss für Wirtschaft, Infrastruktur, Energie, Tourismus und Arbeit bis zum Ende des zweiten Quartals 2022 über den Zwischenstand der Aktivitäten zu unterrichten.

Franz-Robert Liskow und Fraktion

Begründung:

Cyberkriminalität umfasst Straftaten, die sich gegen Datennetze, informationstechnische Systeme oder deren Daten richten sowie solche Straftaten, die mittels dieser Informationstechnik begangen werden. Der finanzielle Schaden durch Cyberkriminalität für die deutsche Wirtschaft wird gemäß dem Branchenverband Bitkom auf 223 Milliarden Euro jährlich geschätzt. Die Schadenssumme ist damit inzwischen mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro jährlich betrug. Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen.

Gemäß Lagebericht des Bundeskriminalamtes sind insbesondere folgende Trends festzustellen, die potenziell eine existenzielle Bedrohung für die betroffenen Unternehmen darstellen:

- Eine steigende Intensität an Ransomware-Angriffen, durch die Daten eines Unternehmens zum Zwecke einer Erpressung verschlüsselt werden. Besonders perfide sind dabei Wiper-Versionen, die keine Funktion für die Entschlüsselung der Daten beinhalten, die Daten folglich irreversibel zerstören.

- Eine zunehmende Professionalisierung der Malware-Programmierung führt zur Verbesserung der Obfuskationsfähigkeit dieser Schadsoftware, wodurch die Spionage oder Manipulation von Unternehmensdaten möglichst lange von Sicherheitssystemen unentdeckt bleiben. Zuletzt wurde die Malware „Emotet“ bundesweit bekannt.

Für die Wirtschaft in Mecklenburg-Vorpommern spielen kleine und mittlere Unternehmen (KMU) eine besondere Rolle. Während der Anteil von Beschäftigten kleiner und mittlerer Unternehmen an allen Erwerbstätigen deutschlandweit bei ca. 70 Prozent liegt, entspricht dieser Anteil in Mecklenburg-Vorpommern 91 Prozent. Gleichzeitig liegen für kleine und mittlere Unternehmen die Hürden zur Digitalisierung im Allgemeinen wie zur Stärkung der IT-Sicherheit im Besonderen höher als in großen Unternehmen, da entsprechend spezialisierte Mitarbeiterinnen und Mitarbeiter häufig fehlen und der Spielraum für Investitionen in die IT-Sicherheit zum Teil geringer ist. Nicht zuletzt mangelt es den Unternehmensleitungen zuweilen an dem notwenigen Bewusstsein für die Risiken durch Cyberkriminalität. Der Trend zum Homeoffice, in dem Mitarbeiter nicht selten von privaten Endgeräten auf das Firmennetzwerk zugreifen, verstärkt das IT-Sicherheitsrisiko seit Beginn der Corona-Krise zusätzlich. Für den Wirtschaftsstandort Mecklenburg-Vorpommern ist es daher unabdingbar, kleine und mittlere Unternehmen gezielt darin zu unterstützen, die notwendigen Kompetenzen zur Abwehr von Cyberkriminalität zu entwickeln.