NACHRICHTEN AG

22. August 2024

Hessen im Kampf gegen Cyberkriminalität: Faeser lobt effektive Strategien

Bundesinnenministerin Faeser lobt Hessens Cyberkriminalitätsbekämpfung und fordert mehr Kompetenzen für das BSI in Bonn.

Wiesbaden – Im Rahmen ihres Besuchs in Hessen äußerte sich Bundesinnenministerin Nancy Faeser (SPD) positiv über die staatlichen Maßnahmen gegen Cyberkriminalität. In den Räumlichkeiten des CyberCompetenceCenters (Hessen3C) in Wiesbaden lobte sie die hessischen Anstrengungen und bezeichnete die Institution als ein gutes Beispiel in der Bekämpfung digitaler Bedrohungen.

Faeser, die gemeinsam mit dem hessischen Innenminister Roman Poseck (CDU) die Sicherheitsstrukturen im Land besuchte, betonte, dass Hessen in diesem Bereich zu den führenden Bundesländern gehöre und die Zusammenarbeit aller staatlichen Ebenen, also Bund, Länder und Kommunen, von großer Bedeutung sei. Diese Koordination sei besonders seit dem Beginn des Ukraine-Konflikts vor zweieinhalb Jahren von wachsender Dringlichkeit.

Hessen3C: Ein wichtiger Akteur

Hessen3C ist seit seiner Gründung vor etwa fünf Jahren eine zentrale Anlaufstelle für die Landesverwaltung, Kommunen sowie für kleine und mittelständische Unternehmen, die mit Cyberangriffen zu kämpfen haben. Die Einrichtung bietet nicht nur Unterstützung im Falle eines Angriffs, sondern auch

Schulungen an, um präventiv vor solchen kriminellen Aktivitäten zu schützen. Diese proaktive Haltung soll helfen, die Risiken zu minimieren und die IT-Sicherheit zu erhöhen.

Ein herausragendes Merkmal von Hessen3C ist die 24-Stunden-Hotline, die betroffenen Kommunen und Unternehmen bei Cyberangriffen sofortige Hilfe leistet. Sie ist im ehemaligen Krankenhaus einer Kaserne in Wiesbaden untergebracht und beschäftigt rund 50 Fachkräfte. Im Notfall kann die Beratungsstelle schnell mit einem mobilen IT-Neustart, ausgestattet mit 20 Laptops, reagieren, um betroffenen Einrichtungen so schnell wie möglich zu helfen.

Die Bedrohung durch Cyberkriminalität

Die Bedrohung durch Cyberkriminalität ist heute verbreiteter und professioneller geworden als je zuvor. Markus Wiegand von Hessen3C wies darauf hin, dass moderne Cyberkriminelle sich nicht mehr auf kriminelle Genies verlassen müssen, um Angriffe durchzuführen. Mit nur einer Kreditkarte können sie Schadsoftware im Darknet erwerben, die für Ransomware-Angriffe verwendet wird. Bei diesen Angriffsformen fordern die Täter Lösegeld für die Entschlüsselung der betroffenen Daten und Systeme.

Während des Besuchs kam auch die Idee zur Sprache, das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn mit erweiterten Kompetenzen auszustatten. Poseck unterstützte dies und betonte die enge Zusammenarbeit zwischen Hessen3C und dem BSI, um die Cyberabwehr weiter zu verbessern. Bereits im April hatte Poseck angedeutet, dass eine mögliche Grundgesetzänderung zur Bekämpfung von Cyberangriffen nicht ausgeschlossen sei.

Faeser unterstrich die außergewöhnliche Rolle, die Cyberkriminalität heute in der deutschen Sicherheitslage spielt. Die Herausforderungen seien enorm, insbesondere in Anbetracht der geopolitischen Entwicklungen und der damit

einhergehenden Risiken im digitalen Raum. In ihrem weiteren Programm besuchte Faeser auch das Bundeskriminalamt (BKA) in Wiesbaden und den Innovation Hub in Frankfurt, wo die hessische Polizei digitale Lösungen entwickelt.

Ein Blick in die Zukunft

Die Entwicklungen im Bereich der Cyberkriminalität sind besorgniserregend. Umso wichtiger ist es, dass Institutionen wie Hessen3C und das BSI gut ausgestattet sind und ihre Kompetenzen erweitern können. Nur durch eine starke Zusammenarbeit auf allen staatlichen Ebenen kann Deutschland gegen die wachsenden Bedrohungen in der digitalen Welt bestehen. Das Engagement von Fachleuten, die bereit sind, ihr Wissen weiterzugeben und Unterstützung zu leisten, wird in Zukunft entscheidend sein, um einen Schritt voraus zu sein und die Sicherheit der IT-Infrastruktur zu gewährleisten.

Die Cyberkriminalität hat in den letzten Jahren ein besorgniserregendes Ausmaß erreicht und stellt nicht nur für Unternehmen, sondern auch für staatliche Institutionen eine erhebliche Bedrohung dar. Laut dem Bundeskriminalamt (BKA) wurden 2022 über 150.000 Fälle von Cyberkriminalität registriert, was einen Anstieg von etwa 9,3 % im Vergleich zum Vorjahr darstellt. Besonders herausstechend sind Ransomware-Angriffe, die auch große Unternehmen und kritische Infrastrukturen betreffen. Die ermittelten finanziellen Schäden belaufen sich jährlich auf mehrere Milliarden Euro. Diese Zahlen verdeutlichen die Dringlichkeit, mit der staatliche Behörden und private Unternehmen ihre Sicherheitsstrategien anpassen müssen.

Die Rolle staatlicher Institutionen

In Deutschland spielen verschiedene staatliche Institutionen eine entscheidende Rolle im Kampf gegen Cyberkriminalität. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die zentrale Anlaufstelle für Fragen der IT-Sicherheit und

arbeitet eng mit Landesbehörden und Fachstellen wie Hessen3C zusammen. Ziel ist es, eine koordinierte und effektive Antwort auf die ständig wachsenden Bedrohungen zu gewährleisten. Dazu gehört auch die Entwicklung von Sicherheitsstandards sowie die Durchführung von Schulungen und Informationskampagnen, um das Bewusstsein für Cyberbedrohungen zu schärfen.

Der Austausch von Informationen zwischen Bund, Ländern und Kommunen ist essenziell, da Cyberangriffe oft grenzüberschreitend agieren. Die Schaffung eines nationalen Cyberabwehrzentrums wird in diesem Zusammenhang immer wieder diskutiert. Eine der größten Herausforderungen bleibt, die rechtlichen Rahmenbedingungen für die Strafverfolgung im digitalen Raum zu verbessern. Aber auch der Schutz sensibler Daten und die Privatsphäre der Bürger müssen gewahrt bleiben.

Statistiken über Cyberangriffe

Nach Angaben des Digitalverbands Bitkom gab es 2023 bisher einen Anstieg von 20 % bei Angriffen auf Unternehmen, wobei 75 % der befragten Unternehmen angaben, in den letzten zwei Jahren Ziel von Cyberangriffen gewesen zu sein. Besonders kleinere Unternehmen stehen oft im Fokus, da sie häufig nicht über die notwendigen Ressourcen verfügen, um sich ausreichend zu schützen. Laut einer Umfrage der IHK (Industrie- und Handelskammer) gaben 72 % der kleinen und mittleren Unternehmen an, dass sie sich verstärkt mit Cybersecurity-Themen auseinandersetzen wollen.

Die Zahlen zeigen deutlich, dass Cyberkriminalität ein ernstzunehmendes Problem ist, das nicht nur technische Angriffe umfasst, sondern auch soziale Manipulation, sogenannte Social Engineering. Diese Art der Angriffe zielt darauf ab, Menschen dazu zu bringen, sensible Informationen preiszugeben. Um dem entgegenzuwirken, sind umfassende Schulungsprogramme und Sensibilisierungsmaßnahmen von großer Bedeutung.

Details