CII-Presseinfo 4/2025: Deep-Dive-Reihe zu Hybriden Bedrohungen & Szenarien
11.06.2025 I FINAL

CII-Deep-Dive: Mittelstand und KRITIS mit Nachholbedarf angesichts hybrider Bedrohungslage

11. Juni 2025 – Die aktuelle Bedrohungslage durch hybride Angriffe auf Unternehmen, Infrastrukturen und Behörden erfordert zusätzliche Vorkehrungen von Unternehmen und Behörden. Neben cybergestützten Angriffsrisiken stehen Aktivitäten durch Drohnen, Sabotage, Desinformation sowie ihre ausländischen Urheber im Fokus. Ein dreiteiliges Deepdive-Paper, dessen erster Teil „Angriffsarten im Überblick" heute durch CII-Intelligence Direktor und Geheimdienstexperte Dr. Christopher Nehring veröffentlicht wurde, gibt Auskunft.

In seltener Einstimmigkeit warnen Nachrichtendienste in Deutschland und Europa derzeit vor einer hybriden Risiko- und Bedrohungslage, die sich gegen nahezu alle Strukturen der öffentlichen Ordnung richtet: Betroffen sind Unternehmen, Einrichtungen der Wissenschaft und Gesellschaft sowie der öffentlichen Verwaltung und ihre Mitarbeitenden. „Angesichts der offenkundigen Bedrohungslage mag es verwundern, wie arglos mancherorts das Thema noch immer behandelt wird" erklärte CII-Forschungsdirektor Prof. Dr. Dennis Kipker.

Bedrohungslage: Vielfalt und Professionalität

Laut CII ist der Umfang an Bedrohungsszenarien, Ausführungsarten und Schadensfolgen durch cybergestützte, hybride Angriffe aktuell so vielfältig wie noch nie. Aufgrund staatlicher Aktivitäten aus dem Ausland würden sie zudem an Professionalität und Ausdauer gewinnen. Aber auch unabhängig davon müssten sich Unternehmens- und Sicherheitsverantwortliche derzeit auf regulatorische Vorgaben der Produkt-, Service-, und Netzwerksicherheit sowie Resilienz Kritischer Infrastrukturen einstellen, die es künftig zu beachten gelte.

Als Reaktion auf diese Gemengelage stellt die neue Deep-Dive-Reihe des CII eine Übersicht an hybriden Bedrohungen und Szenarien zusammen, die praxisnahes Orientierungswissen mit Handlungsempfehlungen kombiniert. „Awarness ist der erste Schritt, um Handlungserfordernisse zu erkennen – und hier gibt es große Nachholbedarfe" so Nehring. In der Publikationsreihe gehe es auch darum, Ross und Reiter möglichst konkret zu benennen, um Lage und Lösungsansätze leichter zu veranschaulichen.

CII-Deep-Dive: Wöchentliche Veröffentlichung

Insgesamt umfasst die neue CII-Reihe drei Ausgaben, die ab heute über die nächsten drei Wochen jeden Mittwoch erscheinen:

- Deep-Dive No 1: Angriffsarten im Überblick (hier ab heute abrufbar),
- Deep-Dive No 2: Drohnenangriffe und -abwehr (hier ab 18.06.2025 abrufbar),
- Deep-Dive No 3: Angreifer im Fokus: Russland (hier ab 25.06.2025 abrufbar).

--

CII-Pressekontakt:
Dr. Michael Littger I Director Strategy & Communication
E-Mail: press@cyberintelligence.institute
Phone (Office): + 49 69 505034 602
Mobile (Office): +151 5843 5718

Über das cyberintelligence.institute (CII): *An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Startups entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein: www.cyberintelligence.institute*