CYBER|NTELLIGENCE
.Institute

CII-Presseinfo 09/2026, 07. September 2026

Pressemitteilung:
Fall Berlin nur die Spitze des Eisbergs: cyberintelligence.institute empfiehlt Sofortprogramm für kommunale Cyberresilienz

Berlin, 07.09.2026 – Der Cyberangriff auf das Berliner Landesnetz und die anschließende Veröffentlichung großer Mengen sensibler Verwaltungs- und Bürgerdaten durch die mutmaßlich russischsprachige Ransomware-Gruppe Rhysida haben die Verwundbarkeit deutscher Verwaltungen im digitalen Raum eindringlich vor Augen geführt. Das cyberintelligence.institute (CII) mahnt nun ausdrücklich zu einer sachlichen, zukunftsgerichteten Aufarbeitung des Vorfalls, da die genauen Ursachen für die Tragweite des Datenlecks und der konkrete Zugangsweg der Angreifer derzeit noch Gegenstand laufender IT-forensischer Ermittlungen sind. Vorschnelle Schuldzuweisungen seien nicht zielführend, entscheidend sei jetzt der Blick nach vorn.

> ***„Es wäre zu kurz gegriffen, den Vorfall allein als Berliner Problem zu behandeln", sagt Prof. Dr. Dennis-Kenji Kipker, wissenschaftlicher Direktor des cyberintelligence.institute. „Berlin ist als Sitz der Bundesregierung zweifellos ein neuralgischer Punkt, an dem außergewöhnlich viele sensible Informationen zusammenlaufen. Doch ein vergleichbarer Angriff auf nahezu jede andere deutsche Großstadt oder Landeshauptstadt hätte mit hoher Wahrscheinlichkeit ähnlich gravierende Folgen gehabt und kann sich ebenso zu jeder Zeit ereignen."***

Hintergrund dieser Einschätzung ist die uneinheitliche Cybersicherheitsarchitektur in Deutschland. Während einige Bundesländer bereits eigene Cybersicherheits- oder IT-Sicherheitsgesetze mit klaren Zuständigkeiten erlassen haben, fehlt es andernorts bislang an vergleichbaren verbindlichen gesetzlichen Grundlagen für Städte und Kommunen. Diese Uneinheitlichkeit erschwert eine flächendeckende Cyberresilienz erheblich.

> ***„Die Cybersicherheitsarchitektur in Deutschland gleicht auf Länder- und Kommunalebene nach wie vor einem Flickenteppich mit schwer überschaubaren Zuständigkeiten", so Kipker weiter. „Der Fall Berlin ist insofern nur die Spitze des Eisbergs eines systemischen Problems, das nahezu alle Städte und Kommunen in Deutschland in unterschiedlicher Ausprägung betrifft."***

Das CII sieht deshalb sowohl kurzfristigen als auch strukturellen Handlungsbedarf als Reaktion auf den Berliner Vorfall. Priorität habe dabei eine transparente, faktenbasierte Krisenkommunikation und Ansprechbarkeit gegenüber Bürgerinnen und Bürgern sowie betroffenen Institutionen. Sie muss Bestandteil eines bundesweites Sofortprogramm für kommunale Cyberresilienz mit klaren Bausteinen werden, das an das kürzlich verabschiedete Bundesprogramm „CyberGovSecure" anknüpft und dieses ergänzt: Eckpunkte sind die verbindliche Verankerung von Cybersicherheit als Leitungsaufgabe in Kommunalverwaltungen, die Schulung von Kommunalpolitiker:innen zur Verbesserung der investiven Maßnahmen in regionale Cybersicherheitskonzepte, die flächendeckende Etablierung fachlich unabhängiger kommunaler Informationssicherheitsbeauftragter, einheitliche Standards für Sicherheits-Management-Prozesse, Meldewege und Notfallkonzepte sowie ausreichend ausgestattete Notfall- -und Kommunikationsteams, die Kommunen und ihre Bürger: innen im Ernstfall schnell und unbürokratisch unterstützen können.

> ***„Es geht nicht darum, jetzt mit dem Finger auf einzelne Verwaltungen zu zeigen“, betont Kipker. „Es geht vielmehr darum, aus diesem Vorfall die richtigen Lehren für ganz Deutschland zu ziehen und jetzt entschlossen in strukturelle Cyber-Resilienz zu investieren, bevor der nächste Angriff eine andere Stadt trifft – mit ähnlich fatalen Konsequenzen wie in Berlin.“***

Weitere Informationen zum Thema finden sich in der Studie „Defizite, Anforderungen und Maßnahmen: Kommunale Cybersicherheit auf dem Prüfstand“, die durch das CII veröffentlicht wurde und unter diesem Link abrufbar ist:
https://cyberintelligence.institute/projekte/cii-whitepaper-kommunale-cybersicherheit-auf-dem-pruefstand

---

Prof. Dr. Dennis-Kenji Kipker steht für ein analytisches Gespräch zur Aufarbeitung des Cybervorfalls und zur Beurteilung seiner Auswirkungen gerne zur Verfügung.

Bitte kontaktieren Sie mich dazu – und für weitere Anliegen oder Bildmaterial – jederzeit gerne.

Mit freundlichen Grüßen
Patrick Teichmann

CII-Pressekontakt
Patrick Teichmann, Leiter Kommunikation
E-Mail: press@cyberintelligence.institute
Mobile: +49 151 55688761

cyberintelligence.institute
Am Kupfergraben 6
10117 Berlin // Germany
www.cyberintelligence.institute

Über das cyberintelligence.institute (CII)
Über das cyberintelligence.institute (CII): An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Startups entwickelt das CII in Frankfurt am Main und Berlin neue Lösungen für eine sichere digitale Zukunft. Kerngedanke sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. 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

---