NACHRICHTEN AG

09. Mai 2025

# Cyberangriff auf Ellwangen: Schulen dicht, Ermittlungen laufen!

Cyberangriffe auf Ellwangen und Stuttgart: Unbekannte Täter greifen IT-Systeme an, während Schulen zur Sicherheit offline gehen.


**Ellwangen, Deutschland** - Am 9. Mai 2025 wurde die Stadt Ellwangen Ziel eines gravierenden Cyberangriffs, der die IT-Systeme der Stadt erheblich beeinträchtigte. Diese Attacke ist Teil einer besorgniserregenden Zunahme von Cyberangriffen auf kommunale Einrichtungen, die in den letzten Jahren beobachtet wurde. Der Oberbürgermeister von Ellwangen, Michael Dambacher, äußerte sich besorgt über die unklare Identität des Angreifers sowie dessen Motive, und es gibt derzeit keine Hinweise auf einen Zusammenhang mit den pro-russischen Hackern, die bereits für einen Angriff auf Stuttgart verantwortlich sind.

Am 30. April 2025 war die Internetseite der Stadt Stuttgart nicht

erreichbar. Der Hackergruppe „NoName057(16)“, die sich zu diesem Angriff bekannt hat, werden pro-russische Hintergründe zugeschrieben. Dieser Angriff auf Stuttgart war ein DDoS-Angriff (Distributed Denial of Service), bei dem die städtischen Server überlastet wurden. Im Gegensatz dazu wurde Ellwangen durch eine Sicherheitslücke in den städtischen Systemen angegriffen.

## Reaktionen und Maßnahmen in Ellwangen

In Reaktion auf den Cyberangriff wurden alle Schulen und Kindergärten in Ellwangen vom Netz getrennt. Diese Maßnahme könnte in Verbindung mit den laufenden Abiturprüfungen stehen, da das Kultusministerium die Prüfungsaufgaben gesichert über verschlüsselte Datenleitungen an die Schulen sendet. Auch die Möglichkeit, dass der Angreifer sensible Daten der Stadtverwaltung abgreifen oder manipulieren wollte, steht im Raum.

IT-Leiter Jürgen Seifer arbeitet gemeinsam mit externen Fachleuten daran, die Sicherheitslücke zu identifizieren und schnellstmöglich zu schließen. Um zukünftigen Angriffen besser gewachsen zu sein, wird eine 24/7-Überwachung installiert, um unautorisierte Zugriffe zeitnah zu erkennen. Zudem werden alle 200 städtischen Server auf schadhafte Dateien gescannt und die Schulsysteme vorübergehend abgeschaltet, um eine gründliche Untersuchung der IT-Sicherheit durchzuführen.

## Hintergrund zu Cyberangriffen

Die Vorfälle in Ellwangen und Stuttgart reflektieren eine breitere Problematik im Bereich der Cybersicherheit. Nach Angaben von Hornet Security ist der Schutz digitaler Daten vor Hacks von zentraler Bedeutung, insbesondere vor dem Hintergrund der gestiegenen Bedrohungslage durch Fernarbeit seit der COVID-19-Pandemie. Cyberangriffe zielen darauf ab, Daten zu stehlen, zu zerstören oder die Dienste von Unternehmen und Institutionen zu unterbrechen.

Die häufigsten Ursachen für solche Angriffe sind menschliche Fehler und Software-Schwachstellen, die von Hackern ausgenutzt werden können. Zu den gängigen Angriffsformen gehören neben DDoS-Attacken auch Malware- und Phishing-Angriffe. Um sich gegen die Vielzahl von Bedrohungen zu wappnen, sind proaktive Maßnahmen und Sicherheitsrichtlinien unerlässlich.

Insgesamt zeigt die Situation in Ellwangen und Stuttgart den dringenden Bedarf an Maßnahmen zur Verbesserung der IT-Sicherheit in öffentlichen Institutionen und unterstreicht, wie wichtig es ist, sich vor möglichen Cyberangriffen zu schützen.

Für weiterführende Informationen zu den Arten von Cyberangriffen und deren Auswirkungen kann **Hornet Security** konsultiert werden.

Für aktuelle Entwicklungen und Maßnahmen in Ellwangen bleibt die Berichterstattung von **Schwäbische Post** zu beobachten.

| Details | |
|---|---|
| **Vorfall** | Cyberkriminalität |
| **Ursache** | Sicherheitslücke |
| **Ort** | Ellwangen, Deutschland |
| **Quellen** | • **www.schwaebische-post.de**<br>• **www.hornetsecurity.com** |