Was tun gegen Cyber-Angriffe?

Immer wieder greifen Hacker die Infrastruktur in Deutschland an. Zum Beispiel sorgen sie dafür, dass Kraftwerke nicht mehr laufen, oder legen Behörden lahm. Um sich zu schützen, hat der Staat neue Strategien entwickelt.

Wer am Morgen des 12. Februar 2025 bei der Bremer Polizei anrief, erreichte niemanden: Russische Hacker hatten den Polizei-**Server** mit Tausenden **Aufrufen** pro Minute lahmgelegt. Es dauerte zwei Stunden, bis der Notruf wieder funktionierte. Noch härter traf es den Landkreis Anhalt-Bitterfeld im Jahr 2021: Seine komplette Internetseite war nach einem Cyber-Angriff für ein halbes Jahr offline.

Die städtische Verwaltung nicht zu erreichen, ist ärgerlich. Wirklich gefährlich werden Cyber-Angriffe aber dann, wenn Krankenhäuser oder Kraftwerke zu ihrem Ziel werden – also **Einrichtungen**, die wir zum Leben dringend brauchen. Insgesamt hat das **Bundeskriminalamt** (BKA) 2024 über 330.000 Cyber-Angriffe gezählt – allerdings schätzt man, dass über 90 Prozent der Fälle nicht angezeigt werden. Und die Täter werden immer besser: „Wir sehen schon eine weiter zunehmende **Professionalisierung**“, so BKA-Präsident Holger Münch.

Um sich vor Cyber-Angriffen zu schützen, arbeiten die Behörden heute mit privaten Unternehmen zusammen. Es gibt inzwischen spezielle Systeme, mit denen sich zum Beispiel **Pipelines**, Kraftwerke oder Bahnstrecken kontrollieren lassen. Mithilfe von **Sensoren** lassen sich etwa **akustische Signale** in der Nähe einer Anlage auf einem Monitor darstellen. Ungewöhnliche Geräusche können ein Hinweis auf einen Angriff sein.

Auch **Künstliche Intelligenz** spielt eine immer größere Rolle – sowohl für die Täter als auch in der Polizeiarbeit. Doch tut man genug, um Cyber-Angriffe zu stoppen? Münch ist kritisch: „Ich glaube, dass wir mittlerweile funktionierende Strategien haben, aber besser und schneller werden müssen.“ Denn viele Verwaltungen und Unternehmen in Deutschland verwenden noch immer zu alte Systeme oder **unterschätzen** die Gefahr aus dem Netz.

Autoren: Marcel Fürstenau, Philipp Reichert

Glossar

Cyber-Angriff, -e (m.) – der Einsatz eines Computerprogramms, um jemandem zu schaden (Verb: angreifen; auch: die Cyber-Attacke)

Hacker, -/Hackerin, -nen (aus dem Englischen) – jemand, der versucht, geheime Informationen von fremden Computern zu bekommen

Infrastruktur (f., nur Singular) – alle Anlagen/Einrichtungen, die man braucht, damit das Leben in einem modernen Staat funktioniert, z. B. Straßen, Krankenhäuser

Aufruf, -e (m.) – hier: das Klicken auf eine Internetseite oder ein Video im Internet

etwas lahm|legen – etwas stoppen; etwas zum Stillstand bringen

Strategie, -n (f.) – ein Plan, wie man vorgeht, um ein bestimmtes Ziel zu erreichen

Server, - (m., aus dem Englischen) – ein zentraler Computer, der mit anderen Computern verbunden ist

Einrichtung, -en (f.) – hier: etwas, was meist von einer öffentlichen Stelle (z. B. dem Staat) zur Nutzung für die Öffentlichkeit gemacht wurde (z. B. ein Krankenhaus)

Bundeskriminalamt (n., nur Singular) – eine Behörde der Polizei, die für die nationale Verbrechensbekämpfung zuständig ist

Professionalisierung (f., nur Singular) – die Tatsache, dass jemand immer besser in etwas wird und keine oder nur noch wenige Fehler macht

Pipeline, -s (f., aus dem Englischen) – eine Leitung, durch die Erdgas oder Öl transportiert wird

Sensor, -en (f.) – ein technisches Gerät, das physikalische und chemische Eigenschaften feststellen und messen kann

akustisches Signal, akustische Signale (n.) – das Geräusch; etwas, was man hören bzw. mit Messinstrumenten anzeigen lassen kann

Künstliche Intelligenz (f., nur Singular) – ein Programm, das selbstständig Dinge erkennen, lernen und entscheiden kann (Abkürzung: KI)

etwas unterschätzen – hier: nicht erkennen, wie schwer ein Problem wirklich ist