Was passiert, wenn plötzlich alle digitalen Lichter ausgehen? Im westlich von Paris gelegenen Département Hauts-de-Seine wurde dieses Szenario am 20. Mai 2025 brutale Realität – und zwar mit voller Wucht.

Digitale Dunkelheit

Am Dienstagmorgen war auf einmal alles still: Keine E-Mails, keine Verwaltungssoftware, kein Zugriff auf interne Kommunikationswege – als hätte jemand den digitalen Stecker gezogen. Die Verwaltung reagierte prompt: Systeme runterfahren, Zugriff blockieren, Schadensbegrenzung.

Die Cyberattacke zwang zentrale Verwaltungseinrichtungen der Städte Nanterre, Boulogne-Billancourt, Levallois-Perret, Neuilly-sur-Seine und dem Wirtschaftszentrum La Défense zum Notbetrieb. Formulare auf Papier, Stempel statt Signatur-Pad – zurück in die digitale Steinzeit.

Kein Einzelfall

Für die Region ist dieser Vorfall leider kein Debüt. Bereits 2023 hatte eine Hackergruppe ein Sicherheitsleck ausgenutzt, was jedoch glimpflich verlief. Im März 2025 jedoch traf ein Ransomware-Angriff das Krankenhaus in Rueil-Malmaison – mit Folgen: OP-Termine mussten verschoben, Patientenakten manuell gepflegt werden. Ein Warnschuss, der offenbar ungehört verhallte.

Jetzt, mit dem Totalausfall der Verwaltung, kommt der Weckruf mit dem Holzhammer.

Ein nationales Phänomen

Frankreichs Kommunen stehen zunehmend im Visier von Cyberkriminellen. Der November 2022 markierte einen weiteren Meilenstein: Der Département Seine-et-Marne wurde Ziel einer ähnlichen Attacke. Die Behörden kappten daraufhin alle Netzverbindungen – das digitale Herz stand still.

Diese Häufung zeigt: Hacker haben die Verwundbarkeit öffentlicher Infrastruktur längst erkannt. Die Digitalisierung der Verwaltung – eigentlich ein Fortschritt – entpuppt sich unter dem Brennglas Krimineller als Einfallstor für digitale Sabotage.

Wer steckt dahinter?

Das bleibt vorerst unklar. Die Behörden haben Anzeige erstattet, die nationale Cybersicherheitsagentur ANSSI wurde eingeschaltet. Was genau gestohlen oder kompromittiert wurde, ist Gegenstand laufender Ermittlungen.

Sicher ist: Die Angreifer wussten, wo es weh tut. Die koordinierte Attacke legt nahe, dass hier keine Amateure am Werk waren. Profis – womöglich mit politischen oder finanziellen Motiven?

Konsequenzen und Chancen

Der Angriff legt offen, wie abhängig unser Alltag inzwischen von funktionierenden IT-Strukturen ist. Bürger können keine Dokumente beantragen, Termine werden gestrichen, Mitarbeiter stehen vor dem Nichts. Und doch: In der Krise liegt auch eine Chance.

Vielleicht braucht es genau diesen Schock, damit sich endlich etwas ändert. Keiner will, dass ein paar Klicks reichen, um ganze Verwaltungen ins Straucheln zu bringen?

Investitionen in IT-Sicherheit dürfen nicht mehr als lästige Pflicht betrachtet werden. Firewalls, Notfallpläne, Schulungen – all das muss Standard sein, nicht Luxus. Es braucht keine weitere Mahnung, sondern klare Handlungen.

Vertrauen und Transparenz

Die Menschen im Département reagieren mit einer Mischung aus Frust und Verständnis. Viele wissen, dass die Angestellten vor Ort ebenso betroffen sind. Doch sie erwarten Aufklärung – und Schutz.

Wie sicher sind unsere Daten? Wer garantiert, dass keine persönlichen Informationen in dunklen Ecken des Internets landen? Die Verwaltungen stehen in der Pflicht, diese Fragen ehrlich zu beantworten – und zwar bald.

Was nun?

Im Moment bleibt vielen nur Geduld. Und vielleicht ein bisschen gesunder Menschenverstand: E-Mails mit verdächtigen Anhängen vermeiden, keine sensiblen Daten an unbekannte

Absender senden – und vor allem wachsam bleiben.

Die Rückkehr zum Normalbetrieb wird dauern. Doch wenn aus diesem Desaster die richtigen Lehren gezogen werden, kann daraus sogar etwas Gutes entstehen. Denn eines steht fest: Die digitale Zukunft kommt – ob wir wollen oder nicht. Aber sicher soll sie sein.

Von Andreas M. Brucker