



Frankreich – das Land der Aufklärung, der Philosophie, der Revolutionen. Und doch stolpert es im Jahr 2025 durch ein digitales Minenfeld. Während draußen auf den Boulevards die Republik stolz ihre Trikolore zeigt, bröckelt im Inneren eine andere Säule des Staates: die digitale Sicherheit.

Man hatte Großes vor. Die Olympischen Spiele in Paris sollten ein Symbol sein. Für Stärke, Weltoffenheit, technische Exzellenz. Aber sie wurden auch zur Bühne für Hackergruppen, Spionageversuche und digitale Sabotage. Was nach Science-Fiction klingt, war bittere Realität: gezielte Angriffe auf Infrastrukturen, Kommunikationssysteme, sogar Krankenhäuser.

Es war, als hätte jemand der Nation den digitalen Stecker gezogen – oder zumindest fest daran gerüttelt.

Natürlich gibt es Gegenmaßnahmen. Frankreich hat verstanden, dass die Bedrohung real ist. Budgets wurden erhöht, Expertenteams gebildet, neue Sicherheitsstrategien entworfen. Doch während die Angriffe raffinierter, koordinierter und globaler werden, wirkt der französische Abwehrkampf manchmal wie ein Duell mit verbundenen Augen.

Manche Behörden agieren schnell – andere träge. Und viele Unternehmen? Sie stecken noch immer in den Kinderschuhen der IT-Sicherheit. Veraltete Systeme, mangelhafte Schulungen, fehlendes Risikobewusstsein. Wer glaubt, Firewalls seien eine Allzweckwaffe, hat den Ernst der Lage nicht begriffen.

Und genau hier liegt das eigentliche Problem: Cyber(un)sicherheit ist längst kein technisches Nischenthema mehr. Sie betrifft uns alle. Jeden Tag. Unsere Daten, unsere Mobilität, unsere Gesundheit – alles hängt am digitalen Tropf. Fällt er aus, kippt das System. Ein Stromausfall war früher ein Ärgernis – heute ist er potenziell lebensbedrohlich.

Besonders bitter: Die Angriffe treffen immer häufiger die Schwächsten. Wenn Krankenhäuser lahmgelegt werden, Patientendaten verschwinden, medizinische Geräte stillstehen – dann ist die Grenze vom digitalen Krieg zur realen Katastrophe längst überschritten. Und dann? Wer trägt Verantwortung? Wer schützt?

Frankreich steht an einem neuralgischen Punkt. Die Gesetzeslage zieht langsam nach, EU-Richtlinien setzen Druck, und das öffentliche Bewusstsein wächst. Doch all das reicht nicht, wenn die Umsetzung weiter so schleppend bleibt. Es fehlt nicht nur an Geld – es fehlt an digitaler Kultur. An Priorität. An Ernsthaftigkeit.



Frankreich hat in der Geschichte oft bewiesen, dass es aus Krisen lernen kann. Die Frage ist: Braucht es erst einen digitalen GAU, bevor sich wirklich etwas ändert?

Vielleicht wäre es an der Zeit, Cybersicherheit nicht als lästige IT-Frage zu behandeln – sondern als nationale Aufgabe. Mit der gleichen Entschlossenheit, mit der man einst für Freiheit, Gleichheit und Brüderlichkeit kämpfte. Denn im Jahr 2025 bedeutet Freiheit auch: sicher sein im Netz.

Oder anders gefragt: Wie frei sind wir, wenn jederzeit jemand von außen die Kontrolle übernehmen kann?

Ein Kommentar von C. Hatty