2024 war für Frankreich kein gewöhnliches Jahr – es war ein Jahr der digitalen und physischen Bedrohungen. Ein Jahr, das wie ein Weckruf klang, laut und unüberhörbar. Über 50 Prozent mehr physische Angriffe auf sensible Einrichtungen. Ein Anstieg der Cyberattacken um satte 60 Prozent. Und das ist nur die Spitze des Eisbergs.

Wenn die Realität wie ein Thriller klingt

Die Zahlen der Direction du renseignement et de la sécurité de la défense (DRSD) sprechen eine deutliche Sprache. Infrastrukturen im Bereich Luft- und Raumfahrt, Künstliche Intelligenz, Quantenforschung oder Tiefseeerkundung wurden gezielt ins Visier genommen – durch fremde Staaten, Hackergruppen und andere Akteure mit dubiosen Motiven.

Général Philippe Susnjara, Chef der DRSD, bringt es auf den Punkt: Die Bedrohungslage ist „hoch“ und in gewissen Bereichen sogar zunehmend. Was das bedeutet? Frankreichs strategische Kompetenzen stehen unter Dauerbeschuss.

Digitale Front: Cyberkriminelle und geopolitische Hacker

Das Bild wird noch düsterer, wenn man die Daten der ANSSI – der nationalen Cybersicherheitsbehörde – hinzuzieht. Dutzende von Angriffen dienten 2024 nicht nur dem klassischen Datenklau, sondern verfolgten perfide Ziele: Spionage, Erpressung, systematische Destabilisierung. Besonders besorgniserregend ist, dass kritische Infrastrukturen wie Energieversorgung, Transportnetze und staatliche Behörden ins Visier gerieten.

Ein besonders sensibles Ziel: die Olympischen Spiele in Paris. Schon Monate vor Beginn wurde deutlich, dass das Großereignis nicht nur sportlich, sondern auch cybersicherheits-technisch ein Ausnahmezustand wird. Die Behörden reagierten mit deutlich verstärkten Maßnahmen – von härterer Zugangskontrolle bis zu digitaler Forensik in Echtzeit.

Desinformation als neue Waffe

Doch nicht nur Malware und Phishing bereiten Sorgen. Auch die gezielte Manipulation von Informationen hat 2024 stark zugenommen. Der Dienst Viginum registrierte über 230 Fälle inauthentischer Informationskampagnen – ein Rekordwert, der die Dimension des Problems verdeutlicht.

Diese digitalen Täuschungen zielen nicht nur auf politische Institutionen, sondern auch auf das gesellschaftliche Gefüge. Sie nutzen soziale Spannungen, polarisieren Debatten, streuen

Zweifel und Misstrauen. Die Methode? Subtil, aber effektiv – wie ein Virus, der sich langsam durch das Meinungsklima frisst.

Internationale Gegenwehr und erste Erfolge

Frankreich hat jedoch nicht einfach zugeschaut. Gemeinsame Aktionen mit internationalen Partnern – etwa gegen die berüchtigte LockBit-Gruppe – führten zu Festnahmen und dem Abschalten von Servern. Ein Erfolg, zweifelsohne. Doch wie bei der Hydra wachsen neue Köpfe nach.

Ein kürzlich veröffentlichter Bericht des Senats empfiehlt daher tiefgreifende Reformen: Mehr Ressourcen für Viginum, neue gesetzliche Rahmenbedingungen für Plattformen wie X, Facebook und TikTok – und mehr Verantwortung für ihre Inhalte. Denn wer Informationskanäle kontrolliert, kontrolliert Meinungen.

Wie sicher ist Frankreich noch?

Die zentrale Frage bleibt: Sind Frankreichs Institutionen und Unternehmen ausreichend gewappnet für diese neue Art der Kriegsführung – jenseits von Panzern und Raketen, aber nicht weniger zerstörerisch?

Es braucht mehr als technische Lösungen. Es braucht ein Umdenken. Cybersicherheit ist längst keine IT-Angelegenheit mehr, sondern Teil der nationalen Verteidigung. Die Erkenntnis ist da – jetzt müssen Taten folgen.

Was können Unternehmen tun?

Mehrschichtige Sicherheitsarchitekturen, regelmäßige Audits, Sensibilisierung der Mitarbeitenden – all das gehört längst zum Pflichtprogramm. Doch der wichtigste Schutz bleibt die Reaktionsfähigkeit. Denn nicht die perfekte Verteidigung, sondern die kluge Schadensbegrenzung entscheidet im Ernstfall über Erfolg oder Misserfolg.

Und manchmal – da hilft auch ein bisschen gesunder Menschenverstand. Etwa, wenn ein verdächtiger Link in der E-Mail landet. Oder wenn ein plötzlich auftauchender „Techniker“ Zugang zum Serverraum verlangt.

Fazit? Kein Platz für Naivität

2024 hat gezeigt: Frankreich ist im Fadenkreuz – nicht nur symbolisch, sondern ganz real.

Wer das ignoriert, handelt fahrlässig. Der digitale Raum ist das neue Schlachtfeld unserer Zeit. Und wer dort ungeschützt ist, verliert mehr als nur Daten.

Andreas M. B.