State of Cybersecurity: Italy Under Attack

Published on 28/08/2025

Italy is at the center of a wave of cyberattacks, with a **14% increase** in the first half of 2025 compared to the previous year. The data, emerging from the **State of Cybersecurity** report by Aused and Certego, reveals an escalation of threats that indiscriminately affect large companies, small and medium-sized enterprises (SMEs), and the public sector. This cross-cutting phenomenon highlights the growing vulnerability of the Italian economic system, making **cybersecurity** a strategic priority for the country.

The Most Affected Sectors and Sources of Attacks

The report's data clearly highlights which sectors are most targeted by cybercriminals. **Manufacturing/Industry** leads the ranking with as many as 2,897 attacks, recording a **20%** increase. This demonstrates how Italian factories, pillars of the economy, have become a primary target. Following closely are **Finance/Insurance** with 2,613 attacks (+20%), a logical target given the value of sensitive data and economic resources they manage. Sectors such as

Fashion/Design, **Chemical/Pharmaceutical**, and **Energy/Environment** have also seen a significant increase in attacks, testifying to a diversification of threats.

The origin of these attacks does not surprise experts. **China** is confirmed as the main source of cyber threats, followed by the **United States**, **Russia**, and **India**. The preferred weapons of hackers remain **malware**, **phishing**, and **social engineering**, techniques that exploit human and technological vulnerabilities to gain access to systems and data.

Vulnerabilities and Defense Strategies

Hackers primarily exploit three gateways to infiltrate corporate systems: the **cloud**, **networks**, and **endpoints**. These paths are difficult to fully protect and are often compromised by abnormal user behavior or suspicious access. In the face of this growing pressure, Aused's analysis underscores the need for an integrated approach that includes **investments in advanced technologies, robust security processes, and staff training**.

The fight against cybercrime requires close **collaboration between the public and private sectors**. Companies must not only strengthen their internal defenses but also contribute to a more resilient national security system, based on information sharing and the adoption of common strategies to counter an invisible but increasingly insidious enemy.

News link: https://www.certego.net/it/blog/whitepaper-state-of-cybersecurity-gennaio-giugno-2025/https://www.certego.net/it/blog/whitepaper-state-of-cybersecurity-gennaio-giugno-2025/