CYBER THREATS TO POLISH BUSINESSES in 2025

LUCY AWARENESS

Poland is one of Europe's top targets for ransomware, phishing, and hybrid cyberattacks — with human error amplifying the risk.

Scale of the Threat

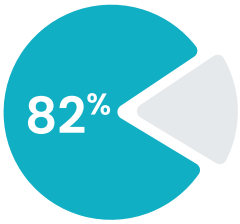
20–50
cyberattacks
daily on critical infrastructure and enterprises

Source: IndustrialCyber, 2025

- **Poland – #1 worldwide target for ransomware (2025)**
  The country most affected by ransomware attacks.
- **41% of companies lack basic protection**
  No antivirus or firewall — an open door for attackers.
- **450+ hacktivist attacks in Q2 2025**
  Business and infrastructure disruptions driven by political and economic motives.
- **$1.7M+ average ransomware recovery cost**
  Each incident costs companies millions of dollars.

Human Factor

82% of data breaches involve human error (clicks, weak passwords, misconfigurations)



Source: Verizon DBIR, 2025

Top Targets in Business & Industry

Healthcare
Attacks disrupted hospital IT, exposing patient data and delaying care

Enterprises
Manufacturing, logistics, and retail among most hit by ransomware

Water utilities
Attempted sabotage of a city's water supply intercepted
Source: Reuters, Aug 2025

Energy sector
Frequent DDoS & intrusion attempts, part of hybrid pressure campaigns

How Businesses Are Responding

- €1B Polish government cybersecurity budget (2025), with business support initiatives
- Growth in managed awareness services for SMEs
- Adoption of risk-scoring & phishing simulation platforms to measure resilience
- Increasing EU–Poland coordination via the Warsaw Call Declaration

Challenges for Polish Organizations

- Low adoption of awareness training compared to EU average
- Overreliance on IT defenses without human-focused measures
- SMEs especially vulnerable – limited budgets, high exposure to supply-chain compromise
- Attribution & response complexity in hybrid attacks

enquiries@lucysecurity.com
www.lucysecurity.com